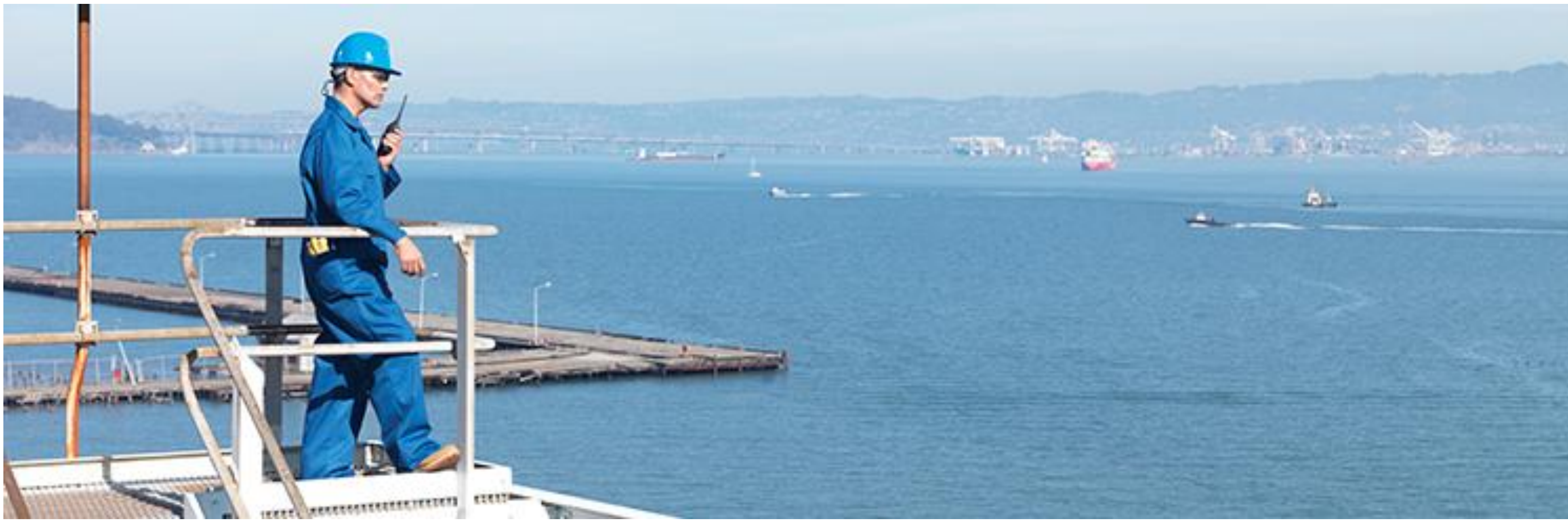


MOTOTRBO™ Connect Plus

MULTI-SITE DIGITAL TRUNKING

System Planner

March 2016

Disclaimer

The information in this document is carefully examined, and is believed to be entirely reliable. However no responsibility is assumed for inaccuracies. Furthermore, Motorola Solutions reserves the right to make changes to any products herein to improve readability, function, or design. Motorola Solutions does not assume any liability arising out of the applications or use of any product or circuit described herein; nor does it cover any license under its patent rights nor the rights of others.

References:

[1] MOTOTRBO System Planner

[2] MOTOTRBO Connect Plus Portable User Guide

[3] MOTOTRBO Connect Plus Mobile User Guide

[4] MOTOTRBO Connect Plus User Guide for XRC Controller

[5] Motorola Quality Standards Fixed Network Equipment Installation Manual R56

Table of Figures and Tables

1 Introduction

The Connect Plus is an integrated digital trunking solution for voice and data, built on the MOTOTRBO system components.

1.1 Purpose

This system planner will enable the reader to understand the features and capabilities of the Connect Plus system, and will provide guidance on how to deploy and configure the system to utilize all its capabilities.

This document should be used in conjunction with the following documentation:
- MOTOTRBO™ System Planner
- MOTOTRBO™ Customer Programming Software (CPS) and related training
- MOTOTRBO™ Connect Plus Option Board CPS[1] and related training
- System workshop/system service training
- Product specification sheets

This system planner has been developed under the assumption that the reader is familiar with the MOTOTRBO technology as well as the different system configurations offered by MOTOTRBO in *digital* mode such as:
- Single Site Repeater
- Talkaround
- IP Site Connect
- Capacity Plus

For a broader discussion and explanation of the underlying TDMA radio technology, system equipment, configurations and features the reader can refer to [1]. This document is structured in such a way that it compares Connect Plus to the other (non-Connect Plus) modes of operation to highlight the advantages as well as identify features that are not offered or required with Connect Plus.

1.2 What's New in System Release R2.5

The R2.5 system release does not impact the Connect Plus infrastructure components – the repeaters, XRC and XRT. The following feature has been added to Connect Plus for this release:

- Vibrating Belt Clip – section 3.1.3.9

1.3 What's New in System Release R1.7 (R2.6.0)

The following main features have been introduced in the current Connect Plus release:

- SIP Telephony – section 2.20
- Permanent Talk Group Registration – section 2.13.12
- Site Talk Group Restriction – section 2.12.10
- Indoor Location – section 2.7.13
- Digital BSI – section 4.2.2
- Extended Text Message – section 2.6.7
- Ignore Emergency Call Activity ("Ignore EM Revert Call RX" configuration option) – section 4.10.20.4

[1] For brevity, the **MOTOTRBO™ Connect Plus Option Board CPS** will be referred to simply as **Connect Plus CPS** from here on.

2 Connect Plus System Feature Overview

2.1 Introduction to Connect Plus

Connect Plus is a single-site or multi-site trunking solution that utilizes MOTOTRBO repeaters and subscribers for its RF components. Because the radios operate in digital mode, a Connect Plus system combines the advantages of MOTOTRBO digital signaling (two voice conversations per repeater, integrated digital features, etc.) with the efficiency of trunking.

A Connect Plus system provides the following capabilities:

- Up to 15 repeaters (30 timeslots) per Connect Plus site.
  - **Note**: The maximum number of traffic slots supported on a system is 770. For example, on a 70-site system installation, *on average* 6 repeaters per site are supported, and on a max size system (250 sites), the *average number* of repeaters per site should not exceed 2. Even though, this limit is not enforced by any system configuration tools, it is strongly recommended **not** to go above it.
- Up to 250 networked RF sites[2]. For multisite network configuration the controllers need to be purchased with such options.
- Dedicated Control Channel timeslot supporting prioritized Busy Queue.
- Most of the same voice & data features available in digital conventional operation.
- Additional features not found in other MOTOTRBO digital modes, including (but not limited to) the following:
  - Dedicated Control Channel Timeslot
  - Validation of Radio IDs and Group ID
  - Validation of the radio's Serial Number, or its Physical Serial Number (PSN)
  - Remote access for user, site, and network management.
  - Prioritized Busy Queue
  - Text Message Mailboxing with Store and Forward Capability
  - Multigroup ID for Voice and Data Calls
  - Ability to update frequency information and Option Board firmware Over-the-air (OTA)
  - In Multi-site network operation, the XRC controllers track each Subscriber Unit (SU) through Connect Plus registration and de-registration messages. This process allows the system to use

[2] When the Multisite Feature is enabled in the XRC, the Connect Plus network supports up to 250 RF sites (Site Numbers 1-250), and up to 5 XRT Gateways (Site Numbers 251-255). When the Multisite Feature is disabled, the XRC does not support networking to other RF sites. It can be connected to one XRT Gateway only (which must be Site number 255).

RF resources efficiently. Calls are only carried at sites where radios are presently registered to the target ID.

2.2 Basic Connect Plus System Components

In addition to the MOTOTRBO repeater and subscriber radios, Connect Plus trunking requires the following basic system components: (For a more detailed discussion of System Components, including optional components, see the "Connect Plus System Components and Topologies" section).

- One XRC Controller per site. Each controller requires a static IP address.
- Each SU in the Connect Plus network must be enabled for Connect Plus operation.
- An Option Board must be installed in each Connect Plus-enabled SU. The Option Board must be loaded with MOTOTRBO™ Connect Plus Option Board firmware, which requires a purchasable license.
- Additional hardware for IP communications:
    - Single-site: At a minimum, this requires an Ethernet switch[3] and cables to connect the XRC Controller and MOTOTRBO repeaters to the switch.
    - Multi-site: In addition to the hardware required for single-site operation, a multi-site network requires additional IP infrastructure. This varies according to network configuration and the type of connections utilized.

2.2.1 XRC Trunking Controller

The XRC Trunking Controller is the central call processing equipment in MOTOTRBO Connect Plus digital trunking solutions. The XRC 9000 is the original Connect Plus trunking controller. The XRC 9100 hardware platform provides the same features as the XRC 9000, along with faster processing, more memory, and external heat dissipation. There are more similarities than differences between the XRC 9000 and XRC 9100[(4)].

Each Connect Plus site requires at least one XRC Controller. If desired, the customer may purchase a second XRC Controller per site to serve as backup to the primary XRC. The secondary XRC can be configured to assume site control if the primary XRC fails, provided that the secondary controller has IP connectivity with its local repeaters. The secondary controller provides backup capability, but it does not increase the number of repeaters and calls that can be managed per site.

The XRC site controller is the core of the Connect Plus infrastructure. The controller's primary responsibilities are outlined as follows:

Via the OTA interface, the XRC communicates with Connect Plus subscribers in order to

- Validate registrations and Call Requests
- Facilitate data transfer

[3] Connect Plus has been tested and validated with the **HP ProCurve 2510-24, 2530-24** and **Cisco Catalyst 3560** switches. For required Ethernet switch performance specifications see the information provided in Appendix E.
[4] For any diagram in the Connect Plus System Planner that depicts an XRC 9000, the device can be either a XRC 9000 or a XRC 9100. Wherever a textual statement or feature description applies to both hardware platforms, the term "XRC" is used.

- Assign RF resources
- Maintain a Busy Queue when no RF resources are available

Via its IP interface, The XRC communicates with all of the site's repeaters in order to

- Assign calls to available timeslots
- Decide which audio packets should be transmitted on the repeater downlink
- Assist repeater with FCC compliance (CWID/BSI, Level I and II Monitoring)

Via its IP interface, the XRC communicates with other network controllers in order to

- Track registrations and de-registrations throughout the Connect Plus network
- Facilitate network call set-up
- Duplicate and forward voice packets to any site where the Target ID is registered
- Route text messages and Location Requests to any site where the Target ID is registered

The XRC provides resources for network management[5] in order to:

- Validate and configure privileges for Connect Plus subscribers
- Configure site and network parameters
- Monitor site RF activity in real time
- Monitor airtime usage and diagnostic information

2.2.2 Control Channel Operation

Each Connect Plus site utilizes a **dedicated** timeslot for Control Channel signaling. The XRC controller uses the Control Channel timeslot for the following operations:

- Receives and responds to registration requests
- Receives and responds to call requests
- Assigns calls to trunk-to timeslots
- Periodically re-sends information for calls-in-progress (thereby supporting late entry)
- Transmits information about surrounding sites (Multi-site operation only)
- Call exchanges that utilize Control Signaling Block (CSBK) Messages occur entirely on the Control Channel timeslot. Sometimes these are called "Command and Control" call features. They include:

[5] Requires the MOTOTRBO™ Connect Plus Network Manager software.

- Radio Check
- Call Alert
- Radio Disable
- Radio Enable
- Private Call confirmation prior to assigning a trunk-to timeslot
- Remote Monitor confirmation prior to assigning a trunk-to timeslot
- Emergency Alert

2.2.3 Control Channel Rollover

The Connect Plus System supports configuration of up to four Control Channel repeaters per site. Only one of these will be active as the Control Channel at any given time. When a repeater is the active Control Channel repeater, Timeslot 1 is used for Control Channel messaging and Timeslot 2 is available for call assignments. When a repeater is configured as a Control Channel repeater, but is not the currently active Control Channel, then both of its timeslots are used for call assignments. To determine which repeater is the site's current Control Channel, connect to the site with the **MOTOTRBO™ XRC Connect Plus Network Manager**[6], and open the Real Time Display.

The Control Channel repeaters must be configured in both the XRC controller (using the Network Manager software) and in the Network Frequency File (configured in the SU using MOTOTRBO Connect Plus CPS). The site's list of Control Channel repeaters as configured in the Network Manager and the Network Frequency File must match exactly. Any and all frequencies flagged as Control Channel must conform to the "Control Channel Requirements" section.

When the controller rolls-over to a different Control Channel repeater, the event is captured in the XRC Event Log. There are three categories of triggers that will cause the XRC to rollover from one Control Channel repeater to another:

1. Scheduled 24-hour rollover: The daily rollover time is configured in the Network Manager.
2. Un-scheduled rollover due to Repeater Failure. This includes the following events:
    a. The XRC boots-up and cannot establish communication with the last-known Control Channel repeater prior to expiration of an internal timer (approximately 65 seconds).
    b. The XRC initially establishes communication with the Control Channel repeater, but subsequently fails to detect a repeater "keep alive" message prior to expiration of an internal timer.
    c. The XRC determines that the current Control Channel repeater has been disabled via a command from the RDAC application.
    d. The XRC boots-up and determines that the last-known Control Channel repeater has a significant active alarm (as defined in Table 2-1).

[6] For brevity, the **MOTOTRBO™ XRC Connect Plus Network Manager** will be referred to simply as Connect Plus Network Manager or as Network Manager from here on.

e. The current Control Channel repeater reports a significant active repeater alarm to the XRC (as defined in Table 2-1). The Repeater Alarm Name and Hexadecimal Alarm Code are captured in the XRC Event Log.

Alarm Name	XPR Repeater Hexadecimal Alarm Code	MTR 3000 Repeater Hexadecimal Alarm Code	SLR Repeater Hexadecimal Alarm Code
Transmitter Alarm	$01	$01	$01
RX Alarm	$02	$02	$02
PA EEPROM Corruption Type 3	Not applicable	$08	Not applicable
PA Voltage Major Alarm	Not applicable	$12	$12
VSWR Major Alarm	$14 (32 MB hardware only)	$14	$14
Transmitter Power Major Alarm (-3dB)	$17 (32 MB hardware only)	$17	$17

Table 2-1 Repeater Alarms that will trigger Control Channel Rollover

It is important to know that if the Control Channel repeater reports any of the above alarms, but the site does not have another Control Channel repeater to rollover to (because there are no other Control Channels configured in the Network Manager, or because all other Control Channels are in error condition) the site will be without a Control Channel. This will cause the XRC to raise the “Control Channel Lost” Controller Alert, and subscriber radios will not be able to use this site in trunking mode until the problem is rectified. The Real Time Display continues to show the site’s last Control Channel repeater (if known). **Note**: Normally, the Control Channel will not roll over to a repeater that is currently experiencing interference. However, the Control Channel will roll over to a repeater that is currently experiencing interference if it is the only available Control Channel repeater.

3. Un-scheduled rollover due to excessive interference on the Control Channel uplink frequency. The operation is as follows:

   a. When the Control Channel repeater detects interference on its uplink frequency that exceeds the interference threshold configured with MOTOTRBO CPS, it sends the XRC a message stating “interference detected”. Meanwhile, the repeater continues to send the XRC any SU messages received on the Control Channel uplink.

   b. When the XRC receives an “interference detected” message from the Control Channel repeater, the controller starts a 30-second debounce timer. This timer is only applied to interference on the Control Channel repeater. If the repeater forwards any valid SU messages prior to sending the “interference clear” message, the XRC will restart its debounce timer upon decoding the valid message. This has the effect of prolonging the debounce timer.

   c. While the controller’s interference debounce timer is running, the controller continues to use the current Control Channel repeater.

   d. The repeater continues to listen for the interference. If the repeater doesn’t detect interference for several seconds, it sends the XRC a message stating “interference clear”.

   e. If the controller receives an “interference clear” message from the repeater prior to expiration of the XRC interference debounce timer, it will continue to use the same Control Channel repeater.

f. If the controller’s interference debounce timer expires, and the controller has not received an “interference clear” message from the repeater, the XRC will look for a different Control Channel repeater:

   i. If the XRC locates another available Control Channel repeater prior to receiving an “interference clear” message, this will cause rollover.

   ii. If the XRC does not locate another available Control Channel repeater prior to receiving an “interference clear” message, the controller will continue to use the same Control Channel repeater.

When the XRC rolls-over to an alternate Control Channel repeater, its preferred choice will be the next repeater in the round-robin list (as determined by the repeater’s Radio ID). This will be the first repeater evaluated by the XRC. However, if Timeslot 1 of the “preferred” rollover repeater is not immediately available, the XRC will evaluate the availability of the other Control Channel repeaters, and it will choose the first repeater that has Timeslot 1 available. For this reason, the next Control Channel repeater can potentially be any other repeater on the Control Channel list.

The scheduled Control Channel Rollover will not occur under the following conditions:

1. At rollover time, there is no available Control Channel repeater (because there are no other Control Channel repeaters on the Network Manager Control Channel list, or because all other repeaters on the list are not checked-in or are in error condition).

2. There is an emergency call in progress at the scheduled rollover time.

Following a scheduled rollover, both timeslots of the former Control Channel repeater will be available for call assignments. Following an un-scheduled rollover, the former Control Channel repeater will not be used for call assignments until it exits from the error condition that triggered the Control Channel change.

It should be noted that Control Channel rollover will cause a temporary loss of site communications by the Connect Plus SU. The radio must temporarily lose signal from the “old” Control Channel repeater before it will search for a new one. When this occurs, the Connect Plus radio looks at all the possible Control Channel frequencies for the last-registered site before it searches any other sites. If it locates an alternate Control Channel for the same site, and if the SU’s Reacquire Timer has not expired, the radio will continue using the site without a new registration. If the SU’s Reacquire Timer has expired, the radio will send a registration to the new Control Channel before it continues using the site. If the radio is in the Busy Queue when the Control Channel rolls-over, it will maintain its “busy state” provided that it locates a different Control Channel repeater for the same site and decodes a subsequent Busy Queue Grant from the new Control Channel prior to expiration of an internal radio timer. If these conditions are not met, the radio exits the “busy state” and the radio user may re-initiate the desired call (once the radio finds a new Control Channel).

If Control Channel rollover is triggered by a scheduled rollover, it is likely that the SU will remain on the same site. This is because the XRC can locate a different (and available) Control Channel repeater prior to taking the old Control Channel repeater off-line. For unscheduled rollovers, the SU may or may not remain on the same site. This is because the triggering event occurs before the XRC has looked for or located a new Control Channel repeater. If the SU searches all remaining Control Channels for the same site and cannot find one (because the XRC hasn’t been able to bring a new Control Channel on-line yet), the SU will start to search the Control Channel repeaters for other network sites (assuming the SU is part of a multisite network). If the SU hears a Control Channel for a different network site with suitable signal strength, the SU will attempt to change sites by transmitting a registration attempt to the new site.

In the General Settings MOTOTRBO CPS provides a repeater codeplug option “Backup Repeater”. This feature is not compatible with Connect Plus and should not be enabled for any repeaters configured for Connect Plus mode.

2.2.4 Control Channel Requirements

- Each Connect Plus site requires a dedicated Control Channel timeslot
- The Control Channel timeslot will always be Timeslot 1 of the Control Channel repeater. Timeslot 2 of the Control Channel is a trunk-to resource for voice and data calls
- The downlink of the Control Channel timeslot transmits continuously. This minimizes the time the SU spends searching for service, and it allows the system to quickly respond to registrations and call requests. Any interruption to this continuous messaging adversely affects system performance. This requirement has the following implications:
    - Control Channel frequency pairs require a Protected Service Area. Non-exclusive licenses such as FB2 or FB6 are not suitable for Control Channel operation.
    - Whenever possible, Analog Base Station Identification (also called CWID) should be sent on trunk channel repeaters only. BSI on the Control Channel repeater interrupts control messaging, which is detrimental to system performance. Digital BSI can be sent on the Control Channel repeater without interrupting control messaging.

2.2.5 Connect Plus Subscriber Radio

In order for a MOTOTRBO subscriber radio to operate on a Connect Plus System, it must meet all of the following requirements.

- The MOTOTRBO radio software version must be compatible with Connect Plus
- A Motorola Option Board must be installed in the SU. Prior to the installation of MOTOTRBO™ Connect Plus Option Board firmware, the radio's Option Board is referred to as a Generic Option Board (GOB). Following installation of Connect Plus software, the Option Board is referred to as Connect Plus Option Board.
- In order for the Connect Plus Option Board to enable its OTA interface and "talk" to the XRC controller, it must first verify that the Connect Plus feature has been enabled in the MOTOTRBO subscriber unit. See "Enabling the Connect Plus Feature" in the "Connect Plus System Design Considerations" section for more information.

2.2.6 Connect Plus Option Board Functions

Connect Plus trunking logic for subscriber radio resides in its Connect Plus Option Board. The Connect Plus Option Board communicates with the MOTOTRBO SU to facilitate the following operations:

- Storing frequency information, and executing frequency changes
- Transmission and reception of Connect Plus control messaging
- Transmission and reception of audio
- Transmission and reception of IP data packets
- Executing Connect Plus features

- Providing ergonomic feedback to the radio user (LED, tones, radio display)

2.2.7 Configuring Connect Plus Subscriber Radios

Configuring a subscriber radio for Connect Plus operation involves the following:

- Using MOTOTRBO™ Customer Programming Software (CPS) to enable “Option Board Trunking” for each Connect Plus personality[7].
- Using MOTOTRBO™ Connect Plus Option Board CPS for advanced configuration of Connect Plus parameters, which includes:
  - Creating Connect Plus Contacts
  - Assigning knob positions
  - Entering Network, Site, & Frequency information
  - Configuring Connect Plus feature options
  - Configuring Connect Plus Menu Operation

2.3 Connect Plus Channel Access

2.3.1 Polite and Impolite Operation

When programming the SU with MOTOTRBO CPS, Connect Plus requires that the Admit Criteria be set to “Always” for every Connect Plus channel. However, this does not mean that the Connect Plus SU will always use “Impolite” Channel Access. In fact, the Connect Plus subscriber radio uses a combination “Polite” and “Impolite” channel access, depending on the specific operation as discussed below:

- Control Channel Registration messages and Call Requests are transmitted impolitely. If the SU does not hear a response within the expected period, it sends retries at a random interval. If the first request was not decoded because it collided with a request from another radio, the random retry interval significantly decreases the chance of two consecutive collisions with the same radio.
- For the first voice transmission on a trunk-to channel, the initiating Connect Plus Option Board assumes the channel is available and will request the radio to transmit accordingly. When the radio receives the Option Board transmit request, it will act on the request per its programmed Admit Criteria. Because the Connect Plus system is in charge of channel assignment, it is unlikely that another radio will already be transmitting on the channel.
- For subsequent voice transmissions on a trunk-to channel, the Connect Plus Option Board acts politely. It will not request the radio to transmit if it is aware that another Connect Plus subscriber is already

[7] See “Connect Plus System Design Considerations” section, for more detailed discussion on MOTOTRBO CPS programming.

transmitting. When the Option Board determines that it can transmit and sends a transmit request to the radio, the operation depends on whether the Enhanced Traffic Channel Access Feature (ETCA) has been enabled in the Connect Plus CPS codeplug. For more information, see Section “Enhanced Traffic Channel Access”.

- When the Connect Plus Option Board requests the radio to transmit IP data packets, the radio always executes such requests in a polite manner. It must ascertain the channel is free prior to transmitting. Because the Connect Plus system is in charge of channel assignment, it is unlikely that another radio will already be transmitting on the channel.

Note: In general, digital trunking systems exhibit slower access times compared to two-way radio communication systems utilizing analog and/or conventional technologies.

2.3.2 Repeater Wake-up Provisioning

Just as in conventional operation, the radio cannot execute a transmit request until it synchronizes with the targeted timeslot. Also as in conventional operation, the radio will attempt to wake-up the repeater (by sending a wake-up message) if it receives a transmit request, but has not yet synchronized with the targeted timeslot. However, the radio rarely has to transmit a wake-up message in Connect Plus operation for the following reasons:

- The Control Channel repeater transmits continuously. This makes the wake-up message unnecessary for the Control Channel.

- When the controller assigns a call to an idle trunk-to repeater, the controller sends an IP message that causes the targeted repeater to activate its downlink for the duration of its SIT timer. By the time the Connect Plus subscriber changes to the assigned channel and timeslot, the repeater will already be transmitting idles. This allows the SU to forego the “wake-up” message and quickly align with the assigned slot.

2.3.3 Enhanced Traffic Channel Access

Enhanced Traffic Channel Access (ETCA) is an enhanced traffic channel access procedure for voice transmissions during Call Hang Time. When enabled, ETCA improves the reliability of voice transmissions by minimizing over-the-air (OTA) collisions when two or more radio users press PTT at the same time (or at nearly the same time) during Call Hang Time. ETCA is a programmable option per Option Board zone in Connect Plus CPS.

The following sub-sections provide additional information on ETCA and non-ETCA traffic channel operation.

<u>Traffic Channel voice transmissions **without** ETCA</u>

During Call Hang Time, any call participant can attempt to key-up. If the Connect Plus Option Board is aware that another call participant has keyed-up first, it operates politely and does not allow its local radio user to transmit on top of the other radio. However, when ETCA is not used, if two or more radios key-up at the same time during Call Hang Time (or at nearly the same time), they will not realize that another radio is also transmitting. In this event, more than one radio may provide the talk permit tone and start transmitting digital voice until the radio user releases PTT. If one of the radios has a significantly stronger signal into the repeater, it may capture the receiver and be heard by most call recipients. Meanwhile the other radio(s) that keyed-up will continue to transmit, but will not be heard. The most likely outcome, however, is that all radios will continue to transmit, but none will be heard due to the RF contention of the transmitting radios. The receiving radios may play garbled audio through the

speaker, or the radio user may hear silence. It is also possible that the repeater may interpret the RF contention as interference or co-channel usage, causing both timeslots of the repeater to be unusable for a period of time.

The user experience of simultaneous voice transmissions during Call Hang Time can be significantly improved by enabling ETCA for all call participants.

Traffic Channel voice transmissions **with** ETCA

When ETCA is enabled in all radios, and when multiple radio users press PTT at the same time (or at nearly the same time) during Call Hang Time, each radio will send a transmit request to the system, but only one radio is allowed to transmit voice. The procedure is as follows: When the radio user presses PTT during Call Hang Time, the radio sends a single burst to the system on the repeater input frequency. The radio then transitions to receive mode and listens for a system response on the repeater output frequency. If the radio receives its burst repeated on the repeater output within an expected period of time, the radio transitions back to transmit mode, plays a talk permit tone for the radio user, and transmits digital voice to the repeater uplink until the radio user de-keys. If the radio does not see its burst repeated on the repeater output within an expected period of time (or if the radio receives a burst from a different radio), the radio plays a talk prohibit tone until the radio user releases PTT. The "losing" radio stays in receive mode and plays the voice of the "winning" radio through the speaker.

ETCA works effectively when there is a small time separation between the multiple key-ups. However, if all requests collide exactly, it is possible that none of the radios will receive a grant and all of the radios will play the talk prohibit tone. The radio user can request the radio to try again by briefly releasing PTT, and then pressing it again. The radio does not automatically retry the transmission on its own.

ETCA Advantages

1. Significantly reduces the incidence of simultaneous voice transmissions when two or more users press PTT at the same time (or nearly the same time) during Call Hang Time.

2. Prevents voice transmission during Call Hang Time when the radio is receiving the repeater transmission, but its transmissions are not reaching the repeater. If the radio's PTT request does not reach the repeater, the radio user will hear a Talk Prohibit tone.

ETCA Disadvantages

1. For traffic channel key-ups during Call Hang Time, ETCA increases the time separation between the PTT press and when the radio starts to transmit voice. This is because the radio switches from transmit mode, back to receive mode (as it listens for the system response), and then back to transmit mode again after receiving its grant.

2. When the radio user presses PTT on the traffic channel, there is a greater period of time that the radio provides no ergonomic feedback as it waits for confirmation of its transmit request. When the radio determines the resolution of its request, it provides the appropriate tone (Talk Permit or Talk Prohibit).

Note: In Connect Plus, ETCA is not used for the first voice transmission in a new call. It is only used for the voice transmissions during Call Hang Time. For this reason, enabling ETCA does not increase the time it takes to start a new voice call from the idle state. It only impacts the subsequent voice transmissions during the same call.

ETCA Limitations

1. Connect Plus does not use ETCA for the first voice key-up during the call – only for key-ups during Call Hang Time. Therefore, it is possible that two or more radios can transmit voice at the same time for the first key-up during the call. This can occur if two or more radios, located at different sites, request to start

a brand new call (on the same Group) at the same time, or a nearly the same time. In this event, two or more requesting radios can simultaneously transmit voice to their respective site controllers during the first key-up in the call. However, due to inter-site arbitration, only one these voice streams will normally be heard by the receiving radios, network-wide.

2. A receiving radio might briefly show the PTT-ID of a transmitting radio, but voice might not be heard through the speaker. This occurs when the system repeats a radio's initial burst, but the same radio's subsequent voice stream doesn't reach the repeater (most likely due to fade by the transmitting radio).

Enabling ETCA in Connect Plus CPS

To enable in ETCA in the Connect Plus radio, check the box labeled "Enable ETCA" on the Connect Plus CPS General Zone Parameters screen. If there are multiple Option Board zones in the codeplug, and if ETCA is desired for any zone, it is strongly recommended to enable the feature for all zones. It is also important to emphasize that the ETCA feature is supported only when the radios of all call participants have been enabled for ETCA.

ETCA supported Call Types

When ETCA is enabled via Connect Plus Option Board programming, it is utilized for key-ups during Call Hang Time for the following types of calls.

1. Group Call

2. Multigroup Call
   Note: Only the call initiator or a wireline console operator is allowed to key-up during the Call Hang Time of a non-emergency Multigroup Call.

3. Emergency Call
   Note: ETCA is not utilized for the very first voice transmission after the user presses the Emergency On button, but will be utilized – if enabled – for subsequent voice transmission by the same radio during the same Emergency Call.

4. Private Call

Note: ETCA is not used for Site All Call because the repeater does not transmit Call Hang Time following a Site All Call voice transmission.

Arbitration Time and ETCA Access Time

The XRC Controller and the XRT Controller Gateway have a configurable setting called "*Arbitration Time*". For Multisite Systems, the Arbitration Time can be configured from 120ms to 300ms. The default setting is 180ms. Although the Arbitration Time is configured per-site, **all sites in the same Connect Plus network must be configured for the same Arbitration Time value**. The Arbitration Time determines how long the system holds on to a received voice transmission prior to routing it to the repeater for transmission (or to the XRT Client application). The Arbitration process has two primary goals; (a) it helps assure that all sites provide the same audio when simultaneous (or near simultaneous) key-ups are started at different sites, and (b) when ETCA is utilized, Arbitration determines which radio receives the grant to continue with its traffic channel voice transmission.

The relationship between the Arbitration Time and the traffic channel access time for an ETCA-enabled radio is as follows: A shorter Arbitration Time value results in faster ETCA access. A longer Arbitration Time value results in slower ETCA access. For most customers, the default Arbitration Time of 180ms is recommended. The

Arbitration Time should only be reduced if the network has excellent connectivity throughout, with little to no network delay. As a general rule, Arbitration Time should only be increased beyond the default setting if network delay is above average.

2.4 Connect Plus Features

2.4.1 Registration & De-Registration

Before a Connect Plus subscriber can make or receive calls on the trunking system, it must successfully register with the XRC controller. Registration is also prerequisite for data services. The radio user doesn't need to do anything except power-up the unit and select a Connect Plus-enabled zone and channel. The SU automatically searches for a site and, upon detecting an acceptable site and signal, sends the registration request. The registration message exchange between the controller and the Connect Plus SU occurs on the site's Control Channel timeslot. The messages used are special Connect Plus CSBKs. Connect Plus does not use the MOTOTRBO Automatic Registration Service (ARS). In fact, MOTOTRBO CPS automatically disables ARS when "Option Board Trunking" is selected for a CPS personality.

The controller receives the Connect Plus registration request and checks three IDs contained in the registration request. These ID's must be configured into the controller's user database before the registration can be successful.

- **Unit ID** (also called Radio ID and User ID): Each radio in the Connect Plus system must have a unique[8] Radio ID, which is programmed into the radio with MOTOTRBO CPS. A record for this ID must be created in the controller's user database, and the Record Status must be set to "enabled".

- **Serial Number authentication or Physical Serial Number (PSN) authentication**: Every Connect Plus Registration validates one of the radio's unique serial numbers. Registration authentication is performed on either the Serial Number, or on the radio's Physical Serial Number (PSN), depending on system and Option Board codeplug configuration. For more information, see section "Serial Number Authentication".

- **Registration Group ID**: For every Connect Plus registration, the registering unit must affiliate with a specific Group ID, known as the Registration Group ID (sometimes called the Selected Group ID). The Registration Group ID for each Connect Plus channel knob position (portable) or channel rocker position (mobile) is selected when programming the SU with Connect Plus CPS. Upon receiving the registration request, the controller checks this ID with its user database. There must be a record for the Group ID in the user database, and the Record Status must be set to "enabled". If the "Site All Call ID" is selected as the Registration Group, it is not necessary to create a record for this group, since it is already hard-coded into the controller.

If all of the IDs are valid in the database, the controller sends an affirmative response to accept the registration. The SU provides a successful registration tone[9] to the radio user, which indicates that the SU is ready to make and receive calls. If any of the IDs are unknown or marked as "disabled", the controller rejects the registration by sending a response that disables the registering unit and causes the radio to provide the "disabled" tone to the radio user. See the section on "Control Channel CSBK Data Calls" for more information on "Disable" and "Enable".

[8] It is allowed to reuse a Connect Plus repeater radio ID (1 – 15) for a subscriber radio, although this is not recommended.
[9] The same tone is used for successful Connect Plus registration and Voice Announcement completion. When a voice announcement and a Connect Plus registration occur at the same time (or nearly the same time), the tone may be heard twice. The Voice Announcement feature is not available for all radio models.

The Connect Plus registration process has two main purposes: (1) It limits system access to authorized users, and (2) It provides the controller with the important information it needs to properly route calls and efficiently utilize RF and IP bandwidth. All of the following events cause a Connect Plus radio to transmit a registration request to the site controller:

- The Connect Plus SU will request registration after power-up.
- The Connect Plus SU will request registration when the radio user selects (or changes) a Connect Plus zone.
- The Connect Plus SU will request registration when it changes sites.
- The Connect Plus SU will request registration when it loses signal from a Connect Plus site, and then reacquires the same site after an extended period of fade.
- The Connect Plus SU will request registration when the radio user changes the position of the channel knob (portable) or the channel rocker (mobile). This requirement assures that the controller will affiliate the SU with the “Registration Talk Group” that has been programmed for each knob or channel rocker position.

The process of de-registration is also important because it tells the controller which SU’s and Talk Groups no longer require system resources. The following events cause the controller to adjust its list of registered units:

- The controller adjusts its registration lists with each new registration request by the SU.
- The controller will de-register the unit from its former site when it registers with a new site.
- The controller de-registers the unit from its previous Talk Group affiliation when the SU registers with a different Talk Group.
- The controller adjusts its registration lists whenever a unit is de-registered from the network. There are two events that cause the controller to de-register a SU from the Connect Plus network:
    - When the Unit is selected to a Connect Plus zone and registered to a site, and the radio user powers the radio down, the SU will automatically send a de-registration message on Control Channel timeslot prior to shutting off. If the controller decodes the message, it de-registers the SU from the network.
    - The controller sends one or more controller-initiated Radio Checks to the SU after a period of inactivity and the SU fails to respond to any of the Radio Check attempts. The purpose of controller-initiated radio check is to identify and de-register units that no longer require system resources. The controller provides three programmable parameters that affect Control Initiated Radio Check:
        - The controller provides a programmable parameter called “SU Inactivity Time”. The timer is set on a site-wide basis, but is tracked for each individual SU. The timer is reset whenever an SU registers, sends a call request, keys-up during a voice call, or acknowledges a Control Channel Message. If the timer expires, the Controller schedules a Controller Initiated Radio Check at the earliest opportunity.
        - When the “SU Inactivity Timer” expires, the Controller will send at least one Controller Initiated Radio Check. Whether it sends additional retries depends on the value configured into the controller’s of “CSBK Call Retries” parameter (0-4). If the controller is programmed for retries, the interval between retries is determined by the “CSBK Call Retry Interval” setting. The target SU must acknowledge the Controller Initiated Radio

Check to remain registered to the site. If the Controller finishes its Radio Check attempt (and any programmed retries), and receives no SU acknowledgement, the controller will de-register the SU from the network and decrement the number of unit's registered to its "Registration Talk Group" by one.

2.4.2 Receiving & Validating Call Requests

The SU sends all Call Requests on the Control Channel timeslot. Upon receiving a Call Request, the controller performs several checks before it responds to the request. Every Call Request contains two Connect Plus IDs – the Source ID and the Destination ID. The Source ID is the Unit ID for the initiating radio. The Destination ID can be another Unit ID or a Group ID, depending on the type of call that is being requested. The controller checks whether there are records for both IDs in the user database, and that both IDs are configured as "enabled". If the Source ID is not present or is "disabled" in the database, the controller denies the call request and disables the initiating unit. If the Destination ID is not present or is "disabled" in the database, or if there are insufficient privileges required for the call type, the controller denies the call request, but it does not disable the initiating unit.

If the IDs are valid, and all required privileges are in order, the controller checks calls currently in progress. The purposes of this check are (1) to see if the Destination ID is already active in a call and (2) for calls requiring a trunk-to timeslot – to see if a resource is currently available. If the controller sees that the Destination ID is already active in call, a response to this effect is returned to the source SU and the radio user will have to try again later. If a trunk-to timeslot is needed, but none is available, the controller informs the source SU that its call has been placed in the Busy Queue. If there are no problems with any of these checks, the controller proceeds with call set-up. The call set-up procedure varies depending on the call type, of which there are different categories for Connect Plus:

- Voice Calls that require no Control Channel acknowledgement from the Destination Radio(s)
- Voice Calls that require Control Channel acknowledgement from the Destination Radio(s)
- CSBK Control Channel Data Calls
- Trunk-to Channel IP Data Calls

2.4.3 Voice Calls with No Control Channel Acknowledgement

Calls in this category include Group Calls, Multigroup Calls, Site All Call (voice), and Network Wide All Call (which utilizes the Site All Call Voice ID).

- **Group Call**: One or more voice transmissions heard by all available radios that are programmed with and registered to the same Talk Group ID. Group Calls are message trunking. At release of PTT the assigned trunk-to timeslot enters the Group Call Hang Time for a period of time determined through repeater programming. During the Group Call Hang Time, any Group member may transmit on the same trunk-to timeslot. If the Hang Time expires with no further transmissions the call ends. Radios already involved in a previous call on another timeslot will not be aware of the Group Call transmission(s).

- **Multigroup Call**: A one-way voice transmission heard by all available radios that are programmed with the same Multigroup ID. To initiate a Multigroup Call, the SU must have the "Multigroup Initiation" privilege on its SU record in the controller database. At release of PTT the assigned trunk-to timeslot enters the Group Call Hang Time for a period of time determined through repeater programming. During the Group Call Hang Time, only the call initiator may transmit again. If the Hang Time expires with no further transmissions the call ends. Radios already involved in a previous call on another timeslot will not be aware of the Multigroup transmission(s).

- **Site All Call (Voice):** A one-way voice transmission heard by all available radios registered to the same site where the transmission occurs. To initiate a Site All Call voice transmission, the SU must have the "Site All Call Initiation" privilege on its SU record in the controller database. At release of PTT the call ends immediately. There is no Call Hang Time. Radios already involved in a previous call on another timeslot will not be aware of the Site All Call transmission(s).

- **Network Wide All Call (NWAC)**: A one-way voice transmission initiated by a device (such as a digital wireline console) that connects to the Connect Plus network via the XRT Gateway. NWAC cannot be initiated by a subscriber radio. NWAC is a best-effort service that utilizes the Site All Call ID. NWAC is transmitted at every network site that has an available RF resource and where the ID is not already in use. Radios already involved in a previous call on another timeslot will not be aware of the NWAC transmission. When a radio receives a NWAC, it is displayed on the receiving radio as a Site All Call. At the end of the NWAC transmission there is no Call Hang Time.

For these call types, the controller sends a Channel Grant assigning the Source and Destination IDs to a trunk-to timeslot. As long as the call is active on the trunk-to timeslot, the controller will periodically re-send the Channel Grant on the Control Channel timeslot. The repeated Channel Grants are sent for the benefit of late-joiners and radios that return to the Control Channel timeslot before the call ends due to fade. Figure 2-1 provides an example of a Group Call Initiation process.

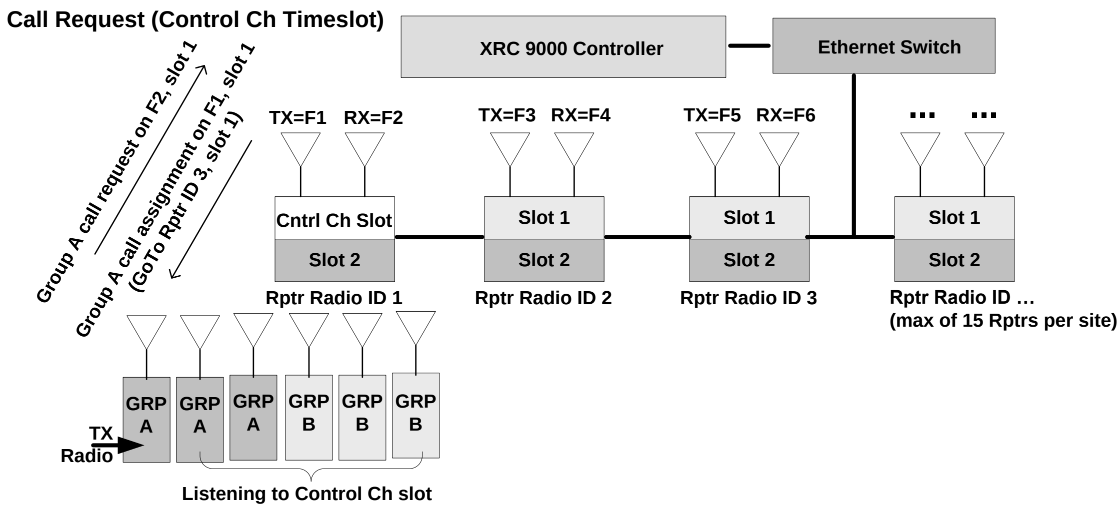


Figure 2-1 Group Call Initiation Example

2.4.4 Voice Calls Requiring a Control Channel Acknowledgement

Calls in this category include Private Calls and Remote Monitor. All of these calls require a Control Channel acknowledgement from the target radio.

- **Private Call:** One or more voice transmissions between two specific radios; the Source SU and the Destination SU. In MOTOTRBO digital conventional operation, Private Calls can be configured as "confirmed" or "unconfirmed" based on MOTOTRBO programming. In Connect Plus, a Private Call always requires a Control Channel acknowledgement from the destination SU before the controller will assign a trunk-to timeslot. In this sense, Connect Plus Private Calls are always confirmed. However, the "Private Call Confirmed" checkbox must <u>not</u> be enabled for any Connect Plus channel via MOTOTRBO CPS. This requirement prevents the participating radios from performing an additional and unnecessary CSBK exchange on the trunk-to timeslot prior to transmitting voice. In order for a Connect Plus Private

Call to take place; all of the following must occur: (a) The Source ID must be enabled for the “Private Call Initiation” privilege on its SU Record in the controller database, (b) The Destination ID must be enabled for the “Private Call Receive” privilege on its SU Record in the controller database, (c) the Destination SU must be registered to a network site and not currently busy in a call, and (d) the Destination SU must acknowledge a Control Channel query before the controller will assign a trunk-to timeslot for the call. Private Calls are message trunking. At release of PTT the assigned trunk-to timeslot enters the Private Call Hang Time for a period of time determined through repeater programming. During the Private Call Hang Time, either party may transmit on the same trunk-to timeslot. If the Hang Time expires with no further transmissions the call ends.

- **Remote Monitor:** The Remote Monitor feature allows a remote user to activate a target radio’s microphone and transmitter for a period of time. A call is silently set up on the target radio, and its PTT is controlled remotely without any indications given to the end user. The duration that the target radio transmits after receiving a Remote Monitor command is set in the target radio through Connect Plus CPS programming. When receiving the Remote Monitor command, the target radio initiates a single, one-way Private Call voice transmission back to the originator of the Remote Monitor command. This feature is used to ascertain the situation of a target radio which is powered-on, but is unresponsive. This is beneficial in a number of situations including theft, incapacity of the radio user, or other situations necessitating a “hands-free” transmission. In order for Remote Monitor to take place; all of the following must occur: (a) The Source ID must be enabled for the “Remote Monitor Initiation” privilege on its SU Record in the controller database, (b) The Destination ID must be enabled for the “Remote Monitor Receive” privilege on its SU Record in the controller database, (c) the Destination SU must be registered to a network site and not currently busy in a call, and (d) the Destination SU must acknowledge a Control Channel query before the controller will assign a trunk-to timeslot for the Remote Monitor transmission.

For these call types, the controller repeats the Call Request CSBK on the Control Channel downlink as a query for the Destination SU. The Destination SU must send acknowledgement on the Control Channel uplink before the call assignment can proceed. If the Control Channel does not receive acknowledgement from the Destination SU, it looks to its programmable “CSBK Call Retry” parameter to see how many times it should resend the Call Request on the Control Channel downlink. If the controller receives no acknowledgement to any of these attempts, it sends a Negative Response to the source SU, which then informs the radio user that the call attempt was not successful. Once the controller receives acknowledgment from the Destination SU, it assigns a trunk-to timeslot for the voice call to proceed.

2.4.5 Other Voice Call Features

The following features are inherent to all Connect Plus Voice Calls:

- **Connect Plus Scan (responding to assigned calls):** When a registered Connect Plus SU is not involved in a call, it listens to all messages transmitted on the Control Channel timeslot. If it decodes any of the call assignments listed below, it responds by moving to the assigned channel and timeslot and joining the call. It will remain on the assigned trunk-to timeslot until the call ends, at which point the Connect Plus SU returns to the Control Channel timeslot. The Connect Plus SU responds to the following call assignments on a first-come, first served basis. In other words, it will not ignore one of these call assignments while it awaits another. Furthermore, while the Connect Plus SU is on the trunk-to timeslot, it will not be aware of (or respond to) Control Channel messages for other calls. Once the Connect Plus SU transitions back to the Control Channel it will respond to the following events:
    - The Connect Plus SU will respond to a call assignment targeting its Unit ID
    - The Connect Plus SU will respond to a call assignment targeting its “Registration Group ID” (sometimes called the Selected Group ID)

- The Connect Plus SU will respond to a call assignment targeting its Multigroup ID (if configured with a Multigroup ID).

- The Connect Plus SU will respond to a call assignment targeting the Site All Call ID. This includes a Network Wide All Call (NWAC), which is initiated by a non-radio device (such as a digital wireline console) and utilizes the Site All Call ID.

- The Connect Plus SU will respond to an Emergency Call targeting its Default Emergency Revert Group ID (if configured for a Default Emergency Revert Group), and if the radio is not configured to Ignore EM Revert Call RX (Ignore Emergency Revert Call Receive).

- The Connect Plus SU will respond to any Group ID that is a currently enabled member of the configurable scan list. For more information on configurable scan options for the Connect Plus SU, see " Group Scan in Connect Plus System"

- **Late entry for voice Calls:** For as long as a voice call continues on a trunk-to timeslot, the Control Channel will periodically repeat the call assignment message on the control channel timeslot. This supports late entry for the following circumstances:
  - A radio that registers after the call started can join the call late.
  - A radio that returned to the Control Channel from another call can join the call late.
  - A radio that faded from the call and returned to the Control Channel will attempt to rejoin the call.

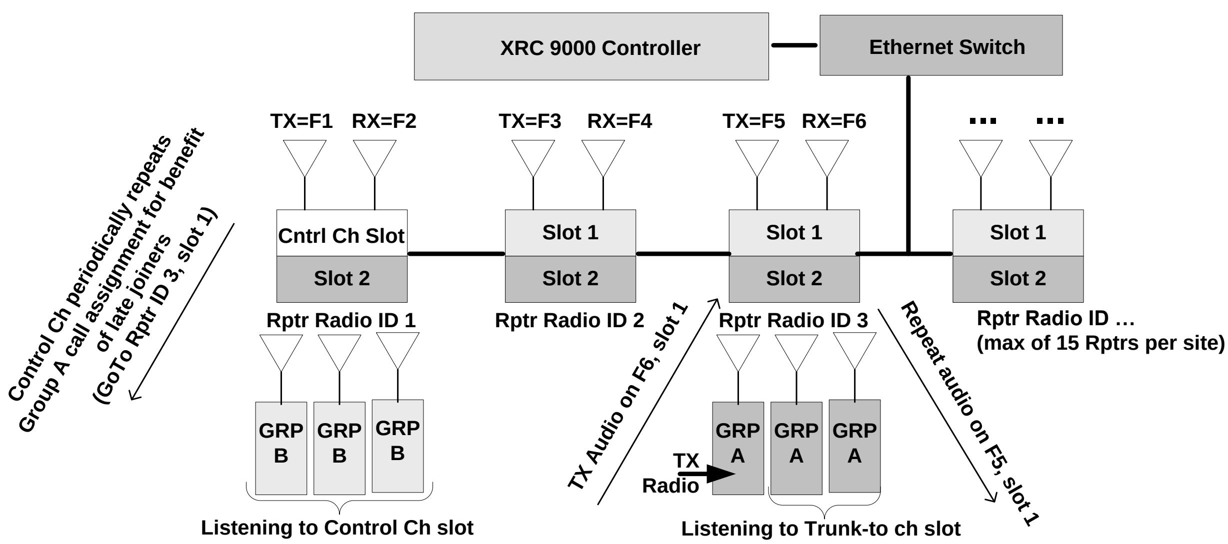


Figure 2-2 Late Entry Example

- **PTT ID and Aliasing:** This feature allows the target radio to identify the originator of a call. If programmed with the Connect Plus CPS, a user friendly alphanumeric name or "alias" can also be displayed. These user friendly aliases are also used when initiating voice calls and digital signaling features. The alias information in the transmitting radio should correspond with the alias information in the receiving radio. The transmitting radio ID is sent over the air and, if there is an alias for that ID in the receiving radio, the receiving radio displays the alias. If no alias is configured at the receiving radio for that ID, then only the transmitting radio's SUID is shown.

- **Call Hang Time**: When radios move to a trunk-to timeslot to participate in a voice call, the Call Hang Time allows an opportunity for talk-back using the same Call ID, without having to return to the Control Channel to request a new call. Besides providing an opportunity for talk-back on the assigned timeslot, the Call Hang Time helps provide continuity to the conversation and prevents the channel from being assigned to another call. The Call Hang Time is configurable per call type for "Group Call", "Private Call" and "Emergency Call". The Call Hang Time values programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Call Hang Time values that have been programmed with the MOTOTRBO Connect Plus Network Manager. The repeater will use the Network Manager-configured values as long as it maintains its connection to the XRC. Connect Plus does support a value of zero for any Call Hang Time. Furthermore, the radio System Administrator must assure that the value chosen for each Call Hang Time setting is programmed the same into each Connect Plus repeater and site network-wide. The Hang Time starts at the end of a voice transmission (either due to release of PTT or fade by the transmitting radio). During the Call Hang Time, other parties in the call may transmit. If the Hang Time expires with no further transmission, the call is considered to be over and radios participating in the call return to the Control Channel timeslot. If a radio user presses PTT after the Hang Time expires, a new voice call will be started using the radio's selected Contact Name, which may be a different ID than the call which just expired. Multigroup Calls use the Group Call Hang Time, but only the initiating radio is allowed to key-up during the Call Hang Time for a Multigroup Call. Site All Call does not use a Hang Time. The call terminates when the first (and only) transmission by the initiating radio is finished.

2.4.6 Control Channel CSBK Data Calls

Calls in this category include Radio Check, Call Alert, Radio Disable, and Radio Enable. They are also known as "Command and Control" call features.

- **Radio Check:** The Radio Check feature checks if a radio is active in a system without notifying the user of the target radio. Besides the Busy LED, there is no other audible or visual indication on the checked radio. The receiving radio automatically and silently responds with an acknowledgement to the initiating radio. This feature is used to discreetly determine if a target radio is available. For example, if a radio user is non-responsive, Radio Check could be used to determine if the target radio is switched on and monitoring the channel. If the target radio responds with an acknowledgement, the initiator could then take additional action such as using the Remote Monitor command to activate the target radio's PTT. If the target radio is not reachable the initiator will receive an indication that the party is not available. The Radio Check message exchange takes place entirely on the Control Channel timeslot. To initiate a Radio Check, the SU must have the "Radio Check Initiation" privilege on its SU record in the controller database. "Controller-initiated Radio Check" is an automatic system feature that the controller uses to determine whether or not an inactive SU should remain registered to the site. Both the SU Inactivity Time and the number of required retries prior to de-registering the SU are programmable settings in the controller.

- **Call Alert:** The Call Alert feature allows a radio user to essentially page another user. To initiate a Call Alert, the SU must have the "Call Alert Initiation" privilege on its SU record in the controller database. When a radio receives a Call Alert, a persistent audible and visual alert is presented to the user. The initiator of the Call Alert is also displayed. If a user is away from his radio at the time of the reception, the alert remains until the user clears the Call Alert screen. If the user presses the PTT while the Call Alert screen is active, he/she starts a Private Call to the originator of the Call Alert provided the radio has Private Call Initiation privilege on its SU Record.

- **Radio Disable:** This feature allows for a radio, typically in a supervisory role, to disable another radio via over the air signaling. The Radio Disable feature can be used to stop an inappropriate use of a radio, or to prevent a stolen radio from making or receiving calls. All messaging related to the Disable feature occurs on the Control Channel timeslot. In order for one radio to remotely disable another, all of the

following must occur: (a) The Source ID must be enabled for the “Disable Command Initiation” privilege on its SU Record in the controller database, (b) The Destination ID must be enabled for the “Disable Command Receive” privilege on its SU Record in the controller database, and (c) the Destination SU must be registered to a network site and not currently busy in a call. When an authorized radio sends the “Disable” command, the controller automatically sets the status on the SU Record to “User Disabled”. This assures that even if the target radio doesn’t hear the Disable Command, it will be disabled by the controller the next time it attempts to register or initiate a call. Upon receiving the Disable Command, the disabled radio sounds the “disabled tone”. If the disabled unit has a display, it shows “Disabled”. A disabled radio is no longer able to make or receive calls in any Connect Plus zone. However, the radio still listens to the Control Channel, responds to certain Control Channel commands, and will search for another site if it loses acceptable signal. Unlike conventional operation, the Disable Command only affects the Connect Plus zones where the command is received. Non-Connect Plus channels are still operable. The radio remains disabled until one of the following occurs: (1) the radio is changed to non-Connect Plus zone, (2) the radio receives a Connect Plus Enable Command in the affected zone, or (3) The SU successfully completes a valid Connect Plus registration. In regards to the latter, the radio will attempt another Connect Plus registration if the user re-cycles power, changes to a Connect Plus zone, or if the radio roams to another Connect Plus site. However, if nothing has changed and SU record is still set to “User Disabled”, the controller will disable the SU again when it attempts to register. The controller will automatically disable a SU if (a) there is no SU Record, or (b) there is an SU Record, but it is set to “Disabled”. Because the SU Record can be set to “User Disabled” via the Network Manager software, the System Administrator can disable any SU via this mechanism. The “Disable Command Receive” privilege only comes into play when the Disable Command is initiated by another radio user.

- **Radio Enable:** This feature allows for a radio, typically in a supervisory role, to Enable another radio via over the air signaling. This assumes, of course, that the target radio was in the disabled condition prior to receiving the Enable command. All messaging related to the Enable feature occurs on the Control Channel timeslot. In order for one radio to remotely Enable another, all of the following must occur: (a) The Source ID must be enabled for the “Enable Command Initiation” privilege on its SU Record in the controller database, (b) The Destination ID must be enabled for the “Enable Command Receive” privilege on its SU Record in the controller database, and (c) the Destination SU must be listening to a network site and within range of Control Channel signaling. When an authorized radio sends the “Enable” command, the controller automatically sets the status on the SU Record to “User Enabled”. This assures that even if the target radio doesn’t hear the Enable Command, it will be enabled by the controller the next time it attempts to register. (The radio will make a registration attempt if (a) the user recycles power, (b) the user changes into a Connect Plus zone, or (b) the radio attempts to Roam to another Connect Plus site.) Upon receiving the Enable Command, the target radio resumes normal operation. Because the SU Record can be set to “User Enabled” via the Network Manager software, the System Administrator can Enable any SU via this mechanism. The “Enable Command Receive” privilege only comes into play when the Enable Command is initiated by another radio user.

For these call types, the controller repeats the Call Request CSBK on the controller channel downlink as a query for the Destination SU. The Destination SU must send acknowledgement on the Control Channel uplink and provide the user ergo associated with the call type (or for Radio Check no ergo indication at all). If the Control Channel does not receive acknowledgement from the Destination SU, it looks to its programmable “CSBK Call Retry” parameter to see how many times it should resend the Call Request on the Control Channel downlink. The interval between retries is determined by another programmable controller parameter, the “CSBK Call Retry Interval”. If the controller receives no acknowledgement to any of these attempts, it sends a Negative Response to the source SU, which then informs the radio user that the call attempt was not successful. If the controller receives acknowledgement from the Destination ID, it repeats the acknowledgement on the Control Channel timeslot. Upon decoding the acknowledgement, the Source SU informs the radio user that the call attempt was successful.

When the SU attempts one of these call types, it will stay with the attempted call until all retries are finished or the call times out. During this time, the radio user will not be able to cancel the current call attempt or initiate a different type of call. To decrease the time that the radio remains in this state, reduce the number of “CSBK Call Retries”.

Note: The “CSBK Call Retry” and “CSBK Call Retry Interval” settings also control the retries when the controller queries the target SU prior to assigning a trunk-to timeslot for a Private Call or Remote Monitor.

2.4.7 Trunk-to Timeslot IP Data Calls

For these types of calls, the controller sends a control channel message that assigns the Destination ID(s) to a trunk-to timeslot for the IP data exchange between the controller and the SU(s). Calls that fall into this category include Text Messages, Location Updates, Packet Data Calls, Generic Data Calls, and Over-the-air File Transfer. For more information, see “Connect Plus Integrated Data”.

2.4.8 Connect Plus Integrated Data

While Connect Plus offers many of the same data features available in other digital modes – such as Text Messaging and Location Updates – there are some differences in configuration and operation, which will be discussed in the sections that follow

Connect Plus Packet Data Call

Connect Plus supports the exchange of “raw” data packets between an XRT Client application and a Non-IP Peripheral device connected to a Connect Plus mobile radio. The packets are called “raw data” because the data payload is generated and interpreted by the two devices at either end of the connection (the XRT Client and the Non-IP Peripheral device). The Connect Plus infrastructure does not understand the meaning of the data. It merely serves as the conduit for transporting the packets.

In order for a Connect Plus radio to send or receive “raw” data packets, the “packet data call” privilege must be enabled on the user record in the XRC/XRT user database **and** the “Enable Packet Data Call” option must be enabled in the Option Board codeplug. In addition, there must be a user record with this privilege enabled that corresponds to the “Data Path ID” registered by the XRT Client.

The characteristics a Packet Data Call depend on the direction of the data packet:

<u>Packet Data Call from Non-IP Peripheral Device (attached to a mobile radio) to XRT Client application</u>

1. Data Type: Currently supports single unbuffered data unit only.

2. Data Protocol: Currently supports Raw Data (user defined) Protocol only.

3. Destination ID: Currently, the Destination ID is an SUID that represents a Data Path registered by an XRT Client. Packet Data Call to a Group ID is not currently supported.

4. Data Payload: Currently supports Raw Data payload up to 472 bytes. (“Max TX PDU Size” must be configured for 500 bytes or larger with MOTOTRBO CPS).

5. Over-the-air direction: Connect Plus subscriber radio to XRC Controller.

6. DMR II Data Transmission: Currently, only DMR II unconfirmed data transmission is supported. Any acknowledgement of received data is the responsibility of the receiving XRT Client application, and must be sent as a separate data call.

7. Queuing: Data packet will be transmitted only if the Connect Plus radio is currently registered to a site, not currently busy with a call, and a traffic channel is immediately available. Busy Queue is not currently

supported. If the Connect Plus radio is not able to transmit the data packet for any of these reasons, it is the responsibility of the Non-IP Peripheral Client application to re-send the packet, if desired.

Packet Data Call from XRT Client application to Non-IP Peripheral Device (attached to a mobile radio).

1. Data Type: Currently supports single data unit only.

2. Data Protocol: Currently supports Raw Data (user defined) Protocol only.

3. Destination ID: Currently, the Destination ID is the SUID of a Connect Plus mobile radio that has an IP Peripheral device attached to it. The Destination ID must be currently registered to a Connect Plus site when the data packet is sent by the XRT Client application. Packet Data Call to a Group ID is not currently supported.

4. Data Payload: Currently supports Raw Data payload up to 472 bytes.

5. Over-the-air direction: XRC Controller to Connect Plus subscriber radio.

6. DMR II Data Transmission: Currently, only DMR II unconfirmed data transmission is supported. Any acknowledgement of received data is the responsibility of the receiving Non-IP Peripheral Client application, and must be sent as a separate data call.

7. Queuing: After accepting a data packet for transmission, the XRC Controller of the SU’s currently registered site will queue the data in the site’s Data Scheduler for up to 210 seconds as it awaits the availability of the Target SU and an RF Resource. If the data cannot be delivered within this time frame, the data is dropped and the Connect Plus system makes a “best effort” to inform the XRC Client application. It is the responsibility of the Client application to re-send the packet, if desired. In a redundant controller configuration, queued packets awaiting OTA delivery are not shared between the “active” and “inactive” XRC Controllers.

Connect Plus Generic Data Call

Connect Plus Generic Data Call is similar to Packet Data Call, but provides greater flexibility to the devices and/or applications that initiate and receive the Generic Data Calls.

Generic Data Call supports the exchange of UDP data packets between an XRT Client application and a destination IP device attached to a radio. The data payload is generated and interpreted by the two devices at either end of the connection. The Connect Plus infrastructure does not understand the meaning of the data. It merely serves as the conduit for transporting the packets.

In order for a Connect Plus radio to send or receive Generic Data Call packets, the “generic data call” privilege must be enabled on the user record in the XRC/XRT user database and the “Enable Packet Data Call” option must be enabled in the Option Board codeplug. In addition, there must be a user record with this privilege enabled that corresponds to the “Data Path ID” registered by the XRT Client.

The characteristics a Generic Data Call depend on the direction of the data packet:

Generic Data Call from the Connect Plus radio (or attached device) to XRT Client application

1. Data Type: Currently supports single data packet transmission.

2. Data Protocol: Requested by the initiating device. Some data protocols are not currently supported for Generic Data Call. Please contact Motorola Solutions Application Developer Program for more information.

3. Destination ID: Currently, the Destination ID is an SUID that represents a Data Path registered by an XRT Client. Generic Data Call to a Group ID is not currently supported.

4. Data Payload: Currently supports data payload up to 512 bytes.

5. Over-the-air direction: Connect Plus subscriber radio to XRC Controller.

6. DMR II Data Transmission: The radio utilizes DMRII confirmed or unconfirmed data transmission, depending on the how the source radio is configured with MOTOTRBO Connect Plus CPS.

7. Queuing: Data packet will be transmitted only if the Connect Plus radio is currently registered to a site, not currently busy with a call, and a traffic channel is immediately available. Busy Queue is not currently supported. If the Connect Plus radio is not able to transmit the data packet for any of these reasons, it is the responsibility of the initiating device or application to resend the packet, if desired.

<u>Generic Data Call from XRT Client application to destination radio (or to a device attached to the destination radio)</u>.

1. Data Type: Currently supports single data packet only.

2. Data Protocol: Requested by the initiating device. Some data protocols are not currently supported for Generic Data Call. Please contact Motorola Solutions Application Developer Program for more information.

3. Destination ID: Currently, the Destination ID is the SUID of a Connect Plus radio. The Destination ID must be currently registered to a Connect Plus site when the data packet is sent by the XRT Client application. Generic Data Call to a Group ID is not currently supported.

4. Data Payload: Currently supports data payload up to 512 bytes.

5. Over-the-air direction: XRC Controller to Connect Plus subscriber radio.

6. DMR II Data Transmission: The XRC Controller utilizes DMRII confirmed or unconfirmed data transmission, depending on the how the user record for the destination radio is configured in the Connect Plus user database.

7. Queuing: After accepting a data packet for transmission, the XRC Controller of the SU’s currently registered site will queue the data in the site’s Data Scheduler (for up to the time-to-live value requested by the initiating XRT Client application) as the controller awaits the availability of the Target SU and an RF Resource. If the data cannot be delivered within this time frame, the data is dropped and the Connect Plus system makes a “best effort” to inform the XRC Client application. It is the responsibility of the Client application to re-send the packet, if desired. In a redundant controller configuration, queued packets awaiting OTA delivery are not shared between the “active” and “inactive” XRC Controllers.

2.4.9 Connect Plus Digital Emergency

Digital Emergency is a set of features that allows a system user to alert other Group members of a crisis situation. Because the type of event that prompts an Emergency varies from one organization to another, it is the responsibility of the company or agency to define the circumstances that constitute an emergency, to train radio users regarding emergency communications procedures, and to conduct drills using the Emergency features.

The XRC controller and the Connect Plus SU treat Emergency Alerts and Emergency Calls in special ways. The controller, for example, gives Emergency Call the highest priority when assigning calls from the Busy Queue (Emergency Alert does not require a trunk-to timeslot, so an Emergency Alert never waits in the Busy Queue). The Connect Plus SU, for its part, allows the Emergency button press in circumstances where would it not allow a normal PTT – such as when the radio is Searching for service and not currently registered to any site. Although the SU will not be able to immediately send the Emergency Alert or Emergency Call Request in this scenario, it will buffer the request until it successfully registers with a Connect Plus site, after which the SU will immediately and automatically transmit the Emergency Alert or Emergency Call Request. When a receiving radio sees that Emergency has been invoked on a Group ID of interest, the Connect Plus SU employs special ergonomics to inform the radio user of the emergency condition.

2.4.9.1 Connect Plus Emergency Features

Just as in other MOTOTRBO digital modes, Connect Plus Emergency is really a set of features designed to facilitate emergency communications.

Connect Plus shares many of the same emergency features as other MOTOTRBO modes. These include the following:

- The ability to signal an emergency condition by pressing a configurable emergency button or pressing an emergency footswitch. The configurable button is available for both portables and mobiles. The footswitch is a purchasable accessory, and is available for mobiles only. The Emergency Alert or Emergency Call can also be triggered automatically via one of the Connect Plus Man Down features. (Man Down is a purchasable option for Connect Plus portable radios. For more information see the section, "Connect Plus Man Down Feature").

- Configurable options to determine SU operation when initiating an Emergency, include the following:

    - A programmable option to configure the Emergency Mode. This setting determines whether the Emergency condition is indicated through Control Channel messaging only (Emergency Alert), or whether the Emergency condition results in the assignment of an Emergency Voice Call (Emergency Call or Emergency Call with voice to follow).

    - A programmable option to start the Emergency Alert or Emergency Call with "regular" or "silent" ergo from the initiating radio. Silent Emergency provides a means to suppress all indications of the emergency status on the initiating radio. This feature is valuable in situations where an indication of an emergency state is not desirable. There are two programmable variations of Silent Emergency; "Silent" and "Silent with voice". For more information on "Silent" and "Silent with voice" operation, see section Emergency Handling Considerations.

    - A programmable option to send voice only upon PTT (Emergency Call), or to start the call with an automatic "Hot Mic" key-up by the initiating radio (Emergency Call with Voice to Follow). When selecting the latter option, the Hot Mic duration is controlled by a programmable timer. An example of an Emergency Call sequence is depicted in Figure 2-3.

- A programmable option to send the Emergency Call on the selected Group ID, or on a specific Emergency Revert Group ID. Emergency Alert is always sent on the SU's Default Emergency Revert Group ID.

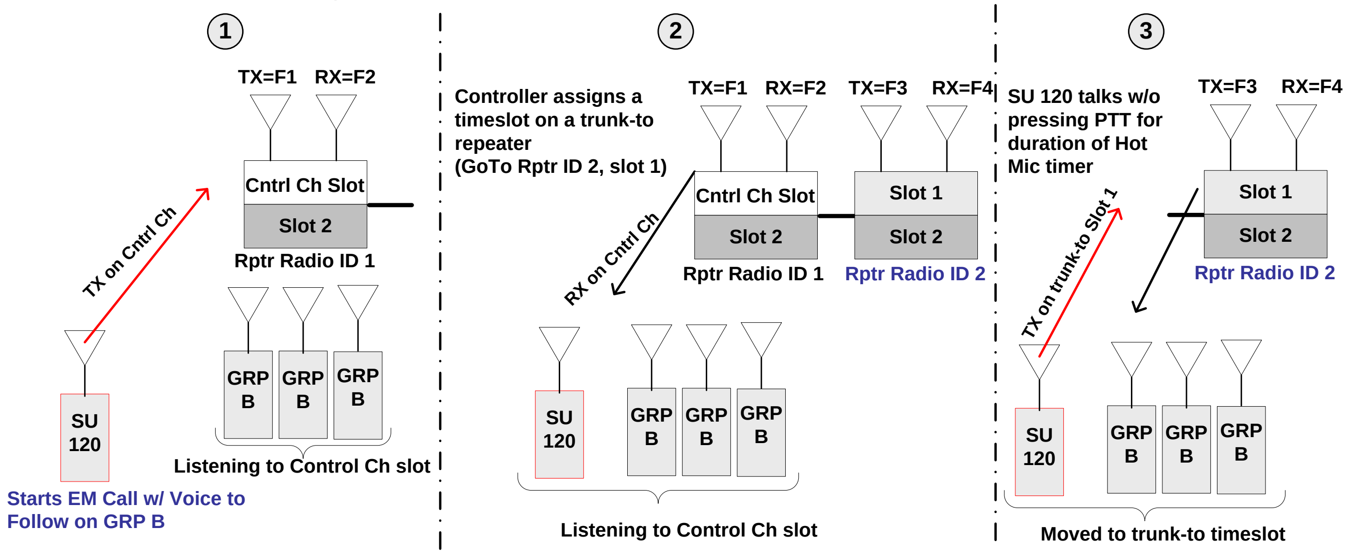


Figure 2-3 Example of Emergency Call with Voice to Follow

- Programmable Options to determine how a radio unit receives an Emergency Alert or an Emergency Call. These options provide the following capability:
  - The ability to provide special ergo for the radio display. The special display ergo can be configured to automatically stop when the Emergency Call ends, or persist until manually cleared by the radio user. Emergency Alert receive ergo (when enabled through Connect Plus CPS) is always persistent until cleared by the radio user.
  - The ability to provide a special Emergency Alert Tone that will persist until manually cleared by the radio user.
  - The ability to forego all special *receive* ergo, so that Emergency Calls will be received in the same manner as other Group Calls. If Emergency Alert receive ergo is disabled through Connect Plus CPS, the radio provides no indication whatsoever of having received an Emergency Alert.
  - The ability to configure the radio to Ignore EM Revert Call RX (Ignore Emergency Revert Call Receive). When this feature is enabled, the radio user can initiate an Emergency Call on a specific Default Emergency Revert Group ID, but the radio will not provide any indication of an Emergency Call (on the same ID) initiated by a different radio, unmute to voice, or allow transmission during that Emergency Call. If any radio is configured to "Ignore EM Revert Call RX", then the Default Emergency Revert Group ID of that radio should not be assigned to a channel selector position in any fleet radio as this can cause undesirable operation for this feature. For more information on how this feature can be used to determine which radios can and cannot respond to an Emergency Call on the Default Emergency Revert Group ID, see section "Emergency Handling Considerations".
- A configurable Emergency Hang Timer that can be set longer than the Group Call Hang Time and Private Call Hang Time, if desired. The Emergency Call Hang Time value that is programmed with MOTOTRBO

CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Emergency Call Hang Time value that has been programmed with the MOTOTRBO Connect Plus Network Manager. The repeater will use the Network Manager-configured value as long as it maintains its connection to the XRC.

- The ability to send a special type of Location Update at the end of the Emergency Alert or Emergency Call. (Just as in other digital modes, this requires the involvement of a Location Tracking Application that must request the emergency update for an “SU of interest” prior to the emergency.)

In addition to the above features shared with other MOTOTRBO digital modes, Connect Plus also provides several emergency enhancements due to fact that it is a networked, trunking system. The Connect Plus emergency enhancements include the following:

- The XRC controller provides an individual acknowledgement to each emergency initiator, and it maintains an accessible list of all emergency initiators. The information – such as call initiator, talk group, and duration – on the ongoing Emergency Calls can be viewed in the Network Manager.
- The XRC controller assigns the repeater and timeslot used for the Emergency Call.
- When no repeater and timeslot is immediately available, the XRC controller places Emergency Calls at the top of the Busy Queue. Emergency Call receives the highest priority when assigning the next available slot. Emergency Alert signaling occurs entirely on the Control Channel timeslot and never has to wait to in the Busy Queue.
- When an SU is configured with a “Default Emergency Talk Group ID” on its user record in the controller database, the XRC assures that Emergency Alerts or Emergency Calls utilizing this ID are routed to the SU’s registered site.
- If the Connect Plus SU receives no response to its Emergency Request from the registered site, it automatically searches for another network site so that it may continue its Emergency attempts.

2.4.9.2 Digital Emergency in Connect Plus vs. non-Connect Plus Mode

While there are many similarities between how Digital Emergency operates in Connect Plus and non-Connect Plus modes, there are also some differences. Most of these differences are due to one of the following reasons; (1) Connect Plus is a trunked radio system where ultimate responsibility for assigning emergency calls lies with the XRC site controller and (2) Emergency operation in the Connect Plus SU is largely controlled by logic residing in the Connect Plus Option Board. For this reason, the SU’s emergency settings are programmed using MOTOTRBO Connect Plus Option Board CPS.

The most important differences between Connect Plus and other MOTOTRBO digital modes are as follows:

Role of Connect Plus Option Board CPS: When the radio user has selected a Connect Plus zone and channel, the emergency operation is determined by the emergency settings that have been configured with MOTOTRBO Connect Plus Option Board CPS. The MOTOTRBO CPS Emergency Settings are not used in Connect Plus. Those settings affect only the non-Connect Plus digital channels. While there are many similarities between the Emergency settings in the two programs, there are also a few differences. These are discussed in greater detail in Section 4.

Role of the XRC Controller: In non-Connect Plus digital modes (e.g. digital conventional), the SU selects the repeater and slot for Emergency based on its MOTOTRBO CPS programming. In Connect Plus, the SU sends an Emergency Call Request to the XRC controller on the Control Channel timeslot. The XRC acknowledges the

emergency, and assigns the repeater and slot for the emergency call from its pool of available channels. If the site is currently busy, the call is placed in the Busy Queue. Emergency calls receive the highest priority when assigning the next available slot.

Emergency Revert: In non-Connect Plus digital modes (e.g. digital conventional), the SU's "Emergency Revert Channel" programmable setting determines not only which Group will be used for the emergency, but also the site, repeater and slot. In Connect Plus mode, the MOTOTRBO Option Board Connect Plus CPS "Default Emergency Revert Group" setting determines which Group ID will be used for emergency, but if the Emergency mode is configured for one of the Emergency Call options, then the repeater and slot is always assigned by the XRC controller of the SU's registered site.

Emergency Alert/Alarm: In non-Connect Plus digital modes (e.g. digital conventional), it is possible to configure the SU to send an Emergency Alarm only, with no Emergency Call to follow. This feature is also available in Connect Plus also, but it is known as "Emergency Alert". In addition to the difference in the feature name, there are several operational differences between Connect Plus Emergency Alert and the Emergency Alarm feature of the non-Connect Plus digital modes.

- In other MOTOTRBO digital modes, the radio can be configured for "Emergency Alarm" (only), "Emergency Alarm with call" or "Emergency Alarm with voice to follow". If configured for Emergency Alarm with call", the radio sends one or more Emergency Alarm messages when the Emergency On button is pressed, and then starts an Emergency Call when PTT is pressed – even if this is a long time after the radio sends the Emergency Alarm. However, if the Connect Plus radio is configured for "Emergency Alert" as the Emergency Mode, this is similar to Emergency Alarm (with no call to follow) operation in other digital modes. If the Connect Plus radio is configured for "Emergency Call" or "Emergency Call with voice to follow" as the Emergency mode, both of these settings are similar to "Emergency Alarm with voice to follow" operation in other digital modes. In Connect Plus both of these Emergency Call modes trigger special receive ergo in a receiving radio (if the receiving radio is so configured), and both of these modes result in the immediate assignment of an Emergency Call (subject to resource availability). When the Emergency Call ends, the radio exits Emergency Mode. In both of the Connect Plus Emergency Call modes, the source radio will make a "hot mic" transmission upon synching with the trunk-to timeslot. The main difference between these two Emergency Call modes is the length of the hot mic transmission. When "Emergency Call" is the Emergency Mode, the radio makes a brief, automatic hot mic transmission (approximately 3 seconds) to start the call on the trunk-to timeslot. The duration of the hot mic transmission is not configurable with Connect Plus CPS, but it can be extended by pressing PTT. If "Emergency Call with voice to follow" is the Emergency Mode, the duration of the hot mic transmission is configurable with Connect Plus CPS.

- In other digital modes, the SU's "Emergency Alarm" *receive* ergo starts when the receiving radio decodes the Emergency Alarm transmitted by the Source SU. In Connect Plus, the "Emergency Alert tone" ergo is prompted by a downlink message sent by the controller. This distinction is fairly minor, however, since the emergency receive ergo on the Connect Plus SU is very similar to non-Connect Plus digital modes.

- In other digital modes, the SU's emergency alarm is acknowledged by an authorized supervisor radio. If the authorized supervisor radio is not listening to the emergency channel, or is not currently within range of the system, the Emergency Alarm can go unacknowledged. In Connect Plus, the XRC controller responds to each and every Emergency Alert and/or Emergency Call Request heard by the system. Over-the-air acknowledgement by other radios is neither required, nor currently supported, in Connect Plus.

- In other digital modes, if the SU transmits all of its configured Emergency Alarm Attempts and does not receive acknowledgement from another radio, the radio indicates "Emergency Alarm Failure". The radio user must press the "Emergency On" button again to re-initiate the process. In Connect Plus, if the SU transmits all of its configured Emergency Attempts and does not receive a controller response, the SU will automatically enter Search mode. Upon locating a site (which might be same site as previously, especially in a single site system or in a multisite network without overlapping site coverage), the SU will

automatically register and start transmitting Emergency Alert messages again. This process continues until the SU receives a controller response to its Emergency Alert, or until the radio user cancels the Emergency.

- In other digital modes a supervisor radio keeps a list of multiple Emergency Alarms from different radios provided that (a) the Alarm is heard by the supervisor radio and (b) the Alarm ergo is not cleared by the radio user. In Connect Plus, a subscriber radio shows the most recently decoded Emergency Alert or Emergency Call only. However, the XRC controller keeps a list of all SU's that have transmitted notification of an emergency condition on its site. The list remains in the controller, even when the emergency is over. If the Connect Plus system has a digital wireline console connected via an XRT Gateway, the console operator will be notified of the Emergency, provided that the console has registered the Group ID used for the Emergency Alert or Emergency Call with the system.

Cancelling Emergency Calls/Alerts and Exiting Emergency Mode: In other digital modes, when an SU is configured for Emergency Call, and when the user presses the "Emergency On" button the radio remains in Emergency Call mode until the user presses the "Emergency Off" button. This can be for seconds, minutes, hours, or even days. Until the "Emergency Off" button is pressed, every press of PTT results in a new emergency call. In Connect Plus, the SU automatically exits Emergency Call mode at the completion of the emergency call. (In other words, after the channel and slot have been assigned and then the Emergency Hang Time expires with no further transmissions.) If the radio user feels that the emergency condition still persists after the Emergency call ends, he/she should press the Emergency button again to re-initiate the process.

There is also a difference in how the Emergency Off button operates in Connect Plus. In other digital modes, the radio user can press Emergency Off at any time, which makes the radio immediately exit Emergency Call (or Emergency Alarm) mode. In Connect Plus, if the radio is configured for Emergency Call or Emergency Call with voice to follow as the Emergency Mode, and if the radio has already transmitted its Emergency Call request to the XRC controller, the radio will stay in Emergency Call mode until the completion of its assigned emergency call ends and the Emergency Call Hang Time expires with no other key-ups. Pressing the "Emergency Off" button during the Emergency Call will not make the radio exit Emergency Call mode any sooner. Neither will it terminate an Emergency Hot Mic transmission prior to expiration of the programmable timer for "Hot Mic Duration". If the radio is configured for Emergency Alert as the Emergency Mode, and if the radio has already transmitted its Emergency Alert request to the XRC controller, the radio will stay in Emergency Alert mode until it receives a response from the controller, or until all of its Emergency Attempts have been sent and the radio enters Search to look for another site. Pressing the "Emergency Off" button while the radio is transmitting its Emergency Alert attempts to the site will not make the radio exit Emergency Alert mode any sooner.

In Connect Plus, the primary function of the Emergency Off button is to prevent the radio from transmitting an Emergency Call or Emergency Alert request in circumstances where the request cannot be immediately sent (such as when the user presses Emergency On while the radio is "Searching"). Once the radio has transmitted an Emergency Call or Emergency Alert Request to a site, the radio user cannot cancel the Emergency Call or Emergency Alert by pressing "Emergency Off". Furthermore, in most normal scenarios it isn't possible to cancel Emergency prior to the SU transmitting the Emergency Call or Emergency Alert Request. This is because the SU normally transmits the Emergency Call or Emergency Alert Request within milliseconds after the radio user presses "Emergency On".

Once the XRC decodes an Emergency Call or Emergency Alert Request, it's not possible to cancel the controller's Emergency Response. If the Emergency Mode is Emergency Call, or Emergency Call with voice to follow, it is best to proceed with the call and let the radio user verbally explain that the situation is not an actual emergency. The Emergency Call can then be allowed to expire with no further transmissions. If the Emergency Mode is Emergency Alert, a designated individual (such as a supervisor or console operator) will likely respond to the Emergency Alert. The radio user can then explain that there is not an emergency situation.

For more information on Connect Plus Emergency Calls, see "Emergency Alert and Emergency Call in Connect Plus" in section 4, which addresses the following topics:

- Making an Emergency Call in Connect Plus
- Emergency Calls on the SU's Multigroup ID
- Programmable Emergency Settings in MOTOTRBO Option Board Connect Plus CPS
- Programmable Emergency Settings in MOTOTRBO Connect Plus Network Manager
- Programming the repeater's Emergency Call Hang Time
- Emergency Handling Considerations
- Conducting Emergency Drills

For more information on Connect Plus Emergency Location Update, see section "Emergency Location Update".

2.4.10 Connect Plus "Man Down" Feature

The Connect Plus Option Board is capable of detecting tilt, movement, and lack of movement. Based on this ability, the Connect Plus Man Down feature can be configured to automatically initiate an Emergency Call from a portable radio when certain conditions are satisfied.

Man Down is a purchasable Connect Plus feature that allows organizations to meet their individual communication needs over and above the standard products feature set. The Man Down features work 'silently' in the background, enabling the user to utilize his/her portable radio as normal. The Man Down feature set is available for portable radio models with and without displays. It is not available for mobile radios.

The Man Down feature set has been developed for a variety of situations, and in particular where radio users work alone, in isolated environments or in hazardous areas. Radio users that can benefit from this feature set include security guards in commercial buildings, forestry workers, agricultural workers, utility workers, and industrial plant workers.

Pre-requisites to utilizing Man Down

The following are pre-requisites for utilizing the Man Down feature set:

1. The Connect Plus Man Down purchasable feature must be enabled in the subscriber unit before the radio can utilize the Man Down feature set. The feature can be purchased through the Motorola Online (MOL) website. After purchasing the feature, an Entitlement ID (EID) will be issued. The EID is used when activating the feature in the subscriber radio with MOTOTRBO CPS. After enabling the Connect Plus Man Down feature with MOTOTRBO CPS, it is necessary to recycle power on the radio. Upon power-up, the Option Board discovers that the Man Down is now enabled.
2. When programming the Connect Plus Option Board with MOTOTRBO Connect Plus CPS, the Emergency Type must be set to Regular, Silent, or Silent with voice. This is configurable per Connect Plus zone.
3. The Man Down parameters must be configured per customer requirements. The Man Down settings are configurable per Connect Plus zone.

How Movement Type can be configured to automatically initiate an Emergency Call

The Movement Type setting determines which movement and/or angle conditions will cause the radio to automatically initiate an Emergency Call:

- **None**: This indicates that no Movement Type has been selected, and the radio will not automatically initiate an Emergency Call due to the Man Down feature set.
- **Tilt Alarm**: When the portable radio is tilted at or beyond the configured Activation Angle, it starts a configurabl*e timer. If the configur*able timer expires, and if the portable radio is still tilted at or beyond the

configured angle, a second timer starts and the radio sounds an Alert Tone (if so configured). If the second timer expires, and if the portable radio is still tilted at or beyond the configured angle, the radio automatically initiates an Emergency Call. The Tilt feature can be used by itself, or in conjunction with the Anti-Movement feature. The Movement feature is not available when Tilt is enabled.

- **Anti-Movement Alarm**: When the portable radio is motionless, it starts a configurable timer. If the configurable timer expires, and if the portable radio is still motionless, a second timer starts and the radio sounds an Alert Tone (if so configured). If the second timer expires, and if the portable radio is still motionless, the radio automatically initiates an Emergency Call. The Anti-Movement feature can be used by itself, or in conjunction with the Tilt feature. The Movement feature is not available when Anti-Movement is enabled.
- **Movement Alarm**: When the portable radio senses movement, it starts a configurable timer. If the configurable timer expires, and if the portable radio is still moving, a second timer starts and the radio sounds an Alert Tone (if so configured). If the second timer expires, and if the portable radio is still in motion, the radio automatically initiates an Emergency Call. The Tilt and Anti-Movement features are not available when the Movement feature is enabled.

When the Connect Plus portable radio automatically initiates an Emergency Call due to one of the Movement Type features, the Emergency Type, Emergency Mode, Emergency Revert Group, the number of Emergency Attempts, and the Hot Mic duration (if applicable) are determined by the Emergency settings configured with Connect Plus CPS for the selected Connect Plus zone.

Note: Acceleration or negative acceleration (deceleration) is detected as movement. Steady, uniform movement over a period of time is not detected as movement, and may be interpreted as lack of movement.

Preventing the radio from automatically initiating an Emergency Call

There are several ways that the radio user can prevent the radio from automatically initiating an Emergency Call due to a Movement Type feature:

1. Correct the triggering event before both the Alarm Tone Delay Time and Alarm Activation Time expire.
    a. If the Tilt feature is the triggering event, return the radio to the vertical position. (The radio doesn't have to be perfectly vertical, but it must be tilted less than the configured activation angle).
    b. If the Anti-Movement feature is the triggering event, move the radio.
    c. If the Movement feature is the triggering event, stop the radio's motion.
2. Turn the Man Down features off via a programmable button and/or Utilities Menu Option.
3. Reset the Man Down features via a programmable button and/or Utilities Menu Option. This stops any active Alert tone and resets the Movement Type timers. It does not turn the Man Down features off.

Audible and Visual Beacon

To assist a search team in the rescue, the radio can be configured to emit an audible and visual beacon after it automatically initiates an Emergency Call due to one of the Man Down features. **Note that beacons are still emitted even if the Emergency Type is set to Silent**. The Beacon feature, which is part of Man Down functionality, has several configurable options.

1. In regards to the type of beacon that will be used, the configurable options are:
    a. No Beacon
    b. Audible Beacon only. The Audible Beacon is a high-pitched, periodic tone that plays approximately once every 10 seconds, but less often if the radio user is talking. The Beacon tone is temporarily suspended while the radio is transmitting.

c. Audible Beacon plus Visual Beacon. If Visual Beacon is enabled, the backlight illuminates for several seconds when the Beacon tone is played.

2. If Audible Beacon is enabled, there is a programmable option to start the Audible Beacon at maximum speaker volume. This affects all audio heard through the speaker. If the Audible Beacon max volume is disabled, then the Audible Beacon volume is determined by the current volume knob setting. (Even if the Audible Beacon starts at max volume, it can still be turned down by the radio user.)
3. Connect Plus CPS provides a programmable button and/or Utilities Menu option that can be used to turn the Beacon feature on and off.
4. Connect Plus CPS provides a programmable button and/or Utilities Menu option that can be used to reset the Beacon. This stops the Beacon without turning the Beacon feature off.

Once the Beacon tone starts, it will continue to periodically play until one of the following occurs; (a) the radio user stops or resets the Beacon by using the programmable button or menu option, (b) radio user changes zones, (c) radio is turned off, or (d) battery expires.

2.4.11 Automatic Fallback

The Connect Plus Auto Fallback feature allows the Connect Plus radio to automatically detect certain failure scenarios where the site repeaters are no longer communicating with the XRC Controller. When the Control Channel repeater stops sending Connect Plus messages, the Connect Plus radio enters Search mode. If the radio detects that its configured Fallback Channel is operating in Fallback mode, the radio will stop searching and monitor its Fallback repeater. While operating on its Fallback Channel, the Connect Plus radio supports non-emergency Group voice call. This allows the radio to communicate with other subscribers that are monitoring the same repeater and timeslot and using the same Talk Group ID. All Call transmissions are also supported in Auto Fallback mode, and will be heard by all radios monitoring the same repeater and slot, regardless of which Group is currently selected on the receiving radio(s). Auto Fallback transmissions are not networked to other repeaters or sites. The feature is not intended to be a long-term failure mitigation solution. Because Auto Fallback is designed to provide short-term, limited communications until the site is repaired, it should be used to supplement (but not to replace) other failure preparedness strategies such as Redundant XRC and Redundant (i.e. multiple) Control Channels.

For a detailed discussion on Auto Fallback, including important configuration guidelines, see the Auto Fallback section (4.6.5), under Fault Management and Redundancy.

2.4.12 Serial Number Authentication

The type of serial number, which the radio sends when authenticating with the Connect Plus system is configurable per subscriber unit – the choices are (a) Serial Number Authentication, or (b) Physical Serial Number Authentication. Serial Number Authentication is the default method. Physical Serial Number Authentication is a highly secure method.

Important Note: The Registration Security method configured in the Connect Plus Option Board Codeplug (using MOTOTRBO Connect Plus CPS) and the authentication method configured in the Connect Plus user record for the same radio (using the MOTOTRBO Connect Plus Network Manager) must match.

<u>Deciding which Registration Security Type to Use</u>
The Registration Security Type determines how the subscriber authenticates with the Connect Plus controller.

Both security types, Serial Number Authentication and Physical Serial Number Authentication, require the same amount of time for the radio to send a Registration Request and to receive a Registration Response.

Serial Number Authentication: This authentication type has been available since the inception of MOTOTRBO Connect Plus and should be satisfactory for most customers. It is the default Registration Security type and the number is shorter than the Physical Serial Number, making it easier to work with. The Serial Number can be obtained by reading the radio with MOTOTRBO CPS, by reading the radio with Connect Plus CPS, from the original factory packaging, or by removing the battery and looking at the back of the radio. This number is not transmitted over-the-air "as is". Instead, the Connect Plus system converts the Serial Number to another number, known as the Connect Plus ESN, for over-the-air transmission. This conversion occurs behind the scenes and is transparent to the end user. When Serial Number Authentication is enabled, the controller will not accept a registration request unless the ESN information transmitted by the SU matches what the controller expects through the programming of the Serial Number field on the Unit Record. If the numbers do not match, the controller sends a registration response to "Disable" the unit.

Physical Serial Number Authentication: This authentication type validates the Physical Serial Number, which is closely tied to the radio's hardware. The radio's Physical Serial Number can be read from the radio by using MOTOTRBO CPS. The number is represented with 64 hexadecimal characters (0-9, A-F). Because the Physical Serial Number contains many characters, the number must be transferred carefully from MOTOTRBO CPS to the Network Manager to avoid lost or incorrect characters. The "copy and paste" method is recommended. When Physical Number Authentication is enabled, the controller will not accept a registration request unless the Physical Serial Number information transmitted by the SU matches what the controller expects through the programming of the Physical Serial Number field on the Unit Record. If the numbers do not match, the controller sends a registration response to "Disable" the unit.

Configuring the Registration Security Type

Before a Connect Plus radio can successfully register with a Connect Plus controller, perform the following steps to select the type of authentication to be used for Registration Security. This is not a complete list of radio configuration instructions.

1. Obtain and record key information about each subscriber radio in the company or organization.
    a. Connect to the subscriber unit with MOTOTRBO CPS and read the radio. The Serial Number and Physical Serial Number (if applicable) are displayed on the Device Information Screen.
    b. Use the copy and paste method to transfer the Serial Number and Physical Serial Number into the Connect Plus user database, or into an intermediary document that can be used to transfer the numbers into the Connect Plus user database.
2. Decide which type of registration authentication should be used, Serial Number authentication or Physical Serial Number Authentication. Serial Number Authentication is the default method. If Physical Serial Number Authentication is desired, this must be enabled with MOTOTRBO Connect Plus CPS as follows:
    a. Read the radio's Connect Plus Option Board codeplug with MOTOTRBO Connect Plus CPS. On the General Settings screen, locate "Registration Security Type".
    b. Select "Physical Serial Number" from the "Registration Security Type" pull-down menu.
    c. When all Connect Plus Option Board configuration is complete, write the codeplug to the radio. Before the radio can successfully authenticate with the system, the Network Manager configuration described in the next step must be also be complete.
3. User the MOTOTRBO Connect Plus Network Manager to connect to a Connect Plus XRC Controller, or use the MOTOTRBO XRT Configuration Tool to Connect to a Connect Plus XRT Gateway. Although either application can be used, it is recommended to use the MOTOTRBO Connect Plus Network Manager when editing user records for radio users.
    a. Select, "Settings→Users" to open the Connect Plus user database.
    b. Locate or create a user record that matches the Radio ID (SUID) of the subscriber radio.

c. Regardless of which type of Registration Security the radio will utilize, enter the radio's Serial Number into the field labeled, "Serial Number". It is highly recommended to use the "copy and paste" method to transfer the Serial Number into the record.

d. If the radio will utilize the Physical Serial Number for Registration Security, then enable (check) the box labeled, "Enable Physical Serial Number Authentication".

e. After enabling Physical Serial Number Authentication, enter the radio's Physical Serial Number into the Physical Serial Number field. Due to the length of the Physical Serial Number (64 hexadecimal characters), it is highly recommended to use the "copy and paste" method to enter the Physical Serial Number into the radio's user record.

f. Complete all necessary configuration on the user record and then "Save" the record to the controller.

g. If all configuration has been completely correctly, the radio will now be able to register with the Connect Plus controller.

Note: When the application user attempts to save a user record containing a Physical Serial Number, the system checks the Physical Serial Number against all other Physical Serial Numbers already in the database. If there is a conflict in any key portion of the Physical Serial Number, the application displays a message that the record cannot be saved due to Physical Serial Number conflict. The message contains the SUID of the user record with the conflicting Physical Serial Number. The application will not allow the record to be saved until the conflict is resolved.

The Physical Serial Number conflict may not be apparent by simply inspecting the Physical Serial Number in the conflicting record. Physical Serial Numbers can be in conflict even though the numbers may not be completely identical. The best way to resolve the conflict is re-enter both Physical Serial Numbers into the Connect Plus user database (exactly as they appear in MOTOTRBO CPS after reading the radios). This will resolve the conflict.

Event Log entries associated with Serial Number/Physical Serial Number Authentication

The XRC Controller and the Network Manager provide two important SUID-specific Event Log messages that are related to authentication type (Serial Number authentication or Physical Serial Number authentication):

- **Physical Serial Number Authentication Expected**: This SUID-specific Event Log entry indicates that the "Enable Physical Serial Number Authentication" box is currently checked on the unit record, but the radio attempted to authenticate using its Serial Number. This is not allowed, and the Controller disables the registration attempt upon detecting this conflict. The discrepancy between the authentication type requested by the radio and the authentication type expected by the controller should be investigated (and resolved) as soon as possible.

- **Serial Number Authentication Expected**: This SUID-specific Event Log entry indicates that the "Enable Physical Serial Number Authentication" box is not checked on the unit record, but the radio successfully authenticated using its Physical Serial Number (which has been configured into user record). In order to facilitate migration from Serial Number authentication to Physical Serial Number authentication, this is allowed. See the next sub-section for more information. However, once the radio is configured with Connect Plus CPS to authenticate by sending its Physical Serial Number, then the Network Manager user should check the "Enable Physical Serial Number Authentication" box as soon as possible. This assures the system is permitting Physical Serial Number Authentication only for this Radio ID.

Migrating from Serial Number Authentication to Physical Serial Number Authentication

This procedure can be used to migrate a Connect Plus radio from Serial Number Authentication to Physical Serial Number Authentication. The procedure assumes that (a) the radio's correct Serial Number has already been configured into the user record in the Connect Plus user database and (b) all key system components have already been upgraded to software that supports Physical Serial Number Authentication:

1. Read the radio's codeplug with MOTOTRBO CPS.
2. Copy the radio's Physical Serial Number, and paste the number into a secure document that also contains the unit's Radio ID (i.e. SUID). The Radio ID is needed to locate the correct unit record in the Connect Plus user database.
3. Connect to the XRC Controller with the MOTOTRBO Connect Plus Network Manager, and open the Unit Record that corresponds to this Radio ID (i.e. SUID).
4. Check the "Enable Physical Serial Number Authentication" box. This activates the Physical Serial Number entry field.
5. Copy the radio's Physical Serial Number from the secure document, and paste the number into the Physical Serial Number entry field.
6. Uncheck the "Enable Physical Serial Number Authentication" checkbox. The Physical Serial Number entry is preserved. After saving the record, the radio is able to authenticate using either its Serial Number or its Physical Serial Number. It will authenticate using its Serial Number until Physical Serial Number Authentication is enabled with MOTOTRBO Connect Plus CPS.
7. Use MOTOTRBO Connect Plus CPS to enable Physical Serial Number as the Registration Security Type, and send the updated Option Board codeplug to the radio. After updating to the new codeplug, the radio will begin authenticating using its Physical Serial Number.
8. As soon as possible, connect to the XRC Controller with the MOTOTRBO Connect Plus Network Manager, and open the Unit Record that corresponds to this Radio ID (i.e. SUID).
9. Check the "Enable Physical Serial Number Authentication" checkbox and save the record. From this point forward, this Radio ID can only authenticate using the Physical Serial Number that corresponds to this record.

2.5 MOTOTRBO CPS Data Configuration

The System Design Section has a thorough discussion of how a Connect Plus radio should be programmed with MOTOTRBO CPS. The following section discusses how MOTOTRBO CPS Data parameters impact Connection operation. Some MOTOTRBO CPS data settings carry through to Connect Plus personalities, operating the same way in Connect Plus as they do in other digital personalities. Other MOTOTRBO CPS data settings affect only non-Connect Plus modes of operation.

Unless specifically stated otherwise, the settings on the following list affect Connect Plus data operation in the same way as they affect other digital modes.

MOTOTRBO CPS Screen	**Setting/Parameter affecting Connect Plus operation**
General Settings	Radio ID. Connect Plus supports Radio IDs in the range of 1 to 16776351. 16776352 through 16776415 are configurable with MOTOTRBO CPS, but must not be used for Connect Plus radios.
General Settings	GPS. The box must be checked for the radio to utilize its GPS receiver. In some models (and depending on how the radio is configured), the radio user can toggle the GPS receiver on or off. When GPS is disabled, the controller may still assign a channel for a location report if requested by the location application, but the radio will not be able to send its location coordinates.
General Settings	TX Preamble Duration (In Connect Plus, the TX Preamble precedes IP data transmissions only. It does not precede Connect Plus

	CSBKs. The TX Preamble should be set to **zero**.
General Settings	Data Enabled Control Station. If this setting is shown, the box must be checked in order for the radio to transmit or receive any type of IP data. This includes text messages, location updates, and over-the-air file transfer.
General Settings	Persistent LRRP Requests. If the radio is used for Connect Plus operation, do not check the “Save” box. This could interfere with Connect Plus operation.
Network Screen	Radio IP. This is usually left at default setting of 192.168.10.1. Connect Plus will still operate correctly if value is changed.
Network Screen	CAI Network. Must be left at default value of 12.
Network Screen	CAI Group Network. Must be left at default value of 225.
Network Screen	Maximum Transmit PDU Size. Must be set large enough to accommodate the largest text message, data message, or LRRP Report transmitted by the radio while operating in a Connect Plus zone. If the radio is capable of sending a 280 character text message, set **Max TX PDU** to at least 750 bytes. Set to 1500 bytes to accommodate maximum possible location report size containing indoor location elements.
Network Screen	Voice Only. If this setting is shown, the box must be **unchecked** in order for the radio to transmit or receive any type of IP data. This includes text messages, location updates, and over-the-air file transfer.
Channel Screen	Compressed UDP Data Header (do NOT enable for Connect Plus personalities). Set “Compressed UDP Header” to “None”. This will not prevent the Connect Plus radio from utilizing the Compressed UDP Data Header when the XRC Controller expects it do so.
Channel Screen	Data Call Confirmed Checkbox (Must be enabled for Connect Plus personalities). This will not prevent the Connect Plus radio from making unconfirmed data calls when the XRC Controller expects it do so.
Indoor Location Screen	This screen is displayed depending on radio model, firmware level, and device features. It is used to enable Indoor Location tracking, to configure the beacon scan timers, and to create a list of Beacon UUIDs the radio will respond to. For more information, see section “Connect Plus Indoor Location Tracking”.

Due to the Connect Plus Option Board’s role in providing data services, there are some MOTOTRBO CPS parameters that affect non-Connect Plus personalities only. The settings listed in the following table are important for other digital modes, but they have no effect on Connect Plus operation, provided that programmable port numbers are not set to ports already used by Connect Plus Option Board. To avoid conflicts with Connect Plus, the programmer must NOT use any of the following ports for the configurable port settings shown below; 4061, 4062, 4063, 4004.

MOTOTRBO CPS Screen	Setting/Parameter that does not affect Connect Plus operation
Network Screen	Telemetry UDP Port
Network Screen	“Forward to PC” checkbox
Network Screen	ARS Radio ID
Network Screen	ARS Radio Port
Network Screen	TMS Radio ID
Network Screen	User Defined UDP Port #1
Network Screen	User Defined UDP Port #2
Network Screen	User Defined UDP Port #3
Text Messages	Text Messages (programmed “Quick Text” messages are entered via Connect Plus CPS, not MOTOTRBO CPS)
Telemetry	Settings on these screen are not used in Connect Plus operation
Channel screen	ARS (grayed-out when Option Board trunking is enabled)

Note: The following data features are not currently supported while the radio is selected to a Connect Plus enabled zone and channel:

- Over-the-air programming for the radio’s main board as configured via MOTOTRBO CPS. (Over-the-air programming for the Connect Plus Option Board is supported).
- Bluetooth Serial Data
- USB HID Data Routing
- IP Data Modem capability

2.6 Connect Plus Text Messaging

2.6.1 Text Messaging Services

In many regards, Connect Plus Text Messaging Service (TMS) operates the same as other MOTOTRBO digital modes. This includes all of the following points:

- A radio user can create a text message in one of two ways; Quick text or limited free-form text messages.
- Connect Plus CPS supports entry of 10 Quick Text Messages.
- The Connect Plus user can send a Text Message to a Text Message Dispatch Call ID, to an individual Connect Plus radio, or to a Connect Plus Group ID.
- When receiving a text message, the user is notified of a new message by an icon, display string, and an audible tone if enabled in the codeplug via the Connect Plus CPS.

- A Connect Plus radio can store up to 30 received or sent text messages at a time.
    - The user is notified once the Inbox and sent folder storage becomes full.
    - Once full, subsequent new messages automatically cause the oldest messages to be deleted.
    - Messages are not deleted when the radio is turned off.
- A user can store up to 10 draft text messages in the Drafts folder at a time.
    - Once full, subsequent new drafts automatically cause the oldest draft(s) to be deleted. A user can opt to Send, Edit, or Delete the drafts in the Drafts folder.
    - The user can opt to Save a text message that is being written or edited to the Drafts folder.
    - If a high priority event causes the radio to exit the text message editing screen, the current text message is automatically saved into the Drafts folder.
    - A draft that is sent is deleted from the Drafts folder and stored to the Sent folder.
- The user can scroll through messages stored in the various Text Message folders, and can select a specific message for various options such as delete, forward, reply, etc. Available options vary by folder.

Non-display and limited display radios have very limited Text Message capability. They can send a Quick Text message (the Quick Text Message, Destination ID, and One-touch-call button assignment must be configured with Connect Plus CPS), but they cannot send a limited free form text message, or receive a text message. The XRC user record, which can be viewed and edited with the Network Manager, has a checkbox labeled, “Text Receive Capable Radio”. The box should be left unchecked when the user record corresponds to a non-display portable or numeric display mobile. When the box is unchecked, the controller will not accept a text message that is targeted to the radio’s individual ID. Regardless of whether the box is checked or not, the radio will receive a text message that is targeted to a Group ID of interest (like other group members), but a non-display portable or numeric display mobile will not display the message, store the message, or notify the user that one has been received.

Note: In the Enhanced Portfolio models, Connect Plus provides greater support for international languages and international characters than is available in the Connect Plus software for previous radio models (i.e. MOTOTRBO Core Platform models). If a Connect Plus enhanced portfolio radio (or a text message application) sends a text message containing certain international characters to a Connect Plus core platform model, the international character(s) may not display as intended in the Connect Plus core platform radio.

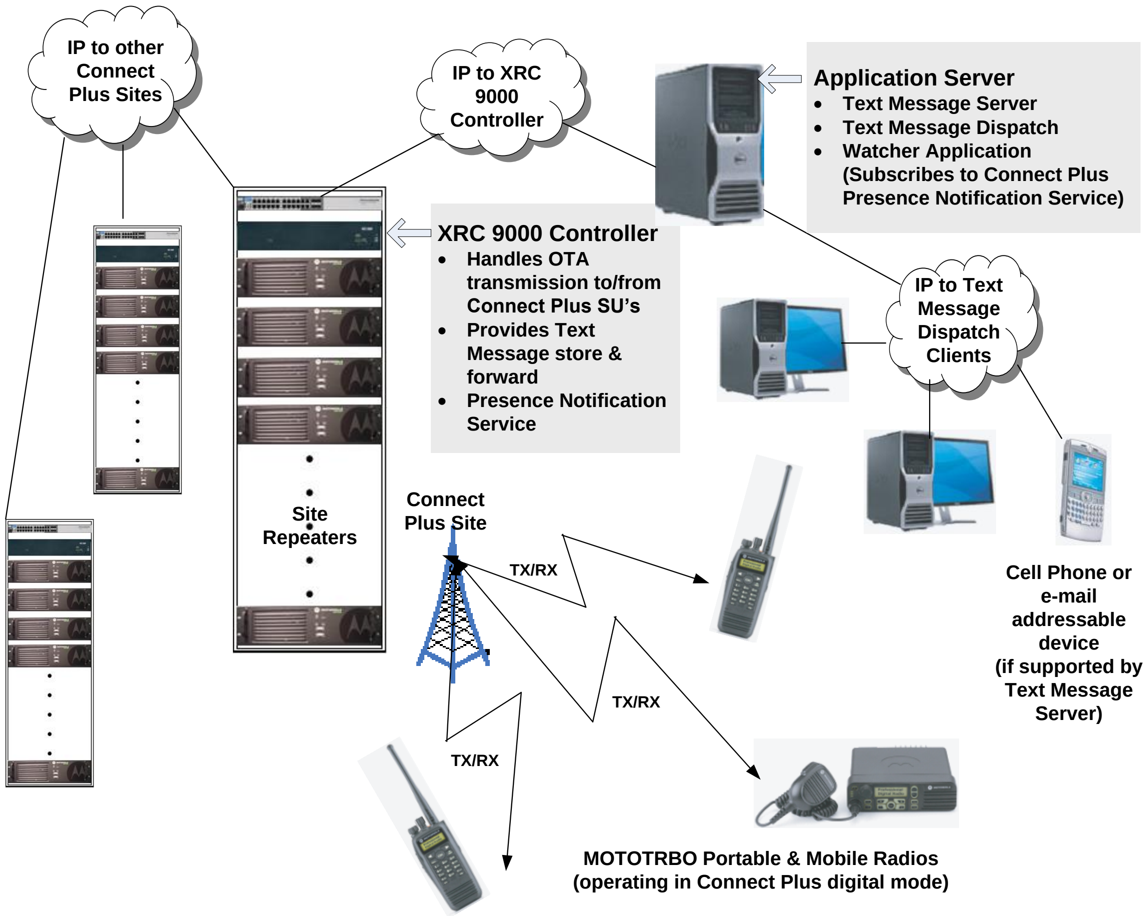


Figure 2-4 Connect Plus Text Messaging Services

Figure 2-4 provides a sample Connect Plus Text Messaging Services configuration. The Text Messaging features are outlined in more detail in the following sections.

2.6.2 Text Messaging features only available in Connect Plus

Connect Plus provides several text messaging features not available in other digital modes:

- **Mail Boxing:** In Connect Plus, text messages are never transmitted directly from one SU to another. Instead, they always pass through the Connect Plus controller. This approach provides significant advantages to the end user. In other digital modes, the text message cannot be successfully sent unless the destination SU is available and listening to the same open channel as the source SU. In Connect Plus, the source SU sends the text message regardless of whether the destination SU is currently available. The controller receives the text message on behalf of the destination SU, places the message in the subscriber's mailbox, and delivers the message at the earliest opportunity. In this regard, the Connect Plus system emulates how text messages are sent on a cellular telephone network. In the controller, each SU has a mailbox that can store up to ten undelivered messages. If a radio or Text Message Service (TMS) Client attempts to send a message to an SU with a full controller mailbox, the source will be notified "mailbox full", and will have to try again at a later time. Any private text message older than the "Text Message Retention Timer" value configured with the Network Manager will be automatically deleted by the controller.

- **Store and Forward Capability:** In a multi-site Network, the text message source does not need to know where in the network the destination SU is currently located. The controller will forward the text message to the registered site and attempt delivery at the earliest opportunity. For a text message to an individual SU, the controller requires OTA acknowledgement from the receiving radio. If OTA acknowledgement is not received, the message is re-queued, and delivery is re-attempted at a later time. If the unit changes sites, the controller will forward the message to the new site to attempt delivery. This process continues until the message is acknowledged, or it times out. Text Messages to a Group ID receive no OTA acknowledgement. They are transmitted (in "unconfirmed" mode) at every network site where the Group ID is registered at the time the message is received by the controller.

- **Text Message to a Multigroup ID:** When the Source radio has been configured with the proper initiation privilege, Connect Plus supports text message transmission to a Multigroup ID. The text message will be sent to all SU's network-wide that share the same Multigroup ID, and who are not already occupied in another call-in-progress. Like all Text Messages to a Group ID, the text message is transmitted "unconfirmed".

- **Text Message to a Site All Call ID:** When the Source radio has been configured with the proper initiation privilege, Connect Plus supports text message transmission to a special Site All Call ID. The text message will be sent to all SU's that are currently registered to the same site where the source radio is located, and who are not already occupied in another call-in-progress. Like all Text Messages to a Group ID, the text message is transmitted "unconfirmed".

2.6.3 Text Message Transmission & Delivery

In other MOTOTRBO digital modes, a Text Message to a Group ID is always sent "unconfirmed" and a Text Message to an Individual (Unit) ID can be sent "confirmed" or "unconfirmed", depending on CPS programming. Connect Plus also uses "unconfirmed" delivery for Text Messages to a Group ID, but it always uses "confirmed" delivery for individual ID's. For this reason, the "Data Call Confirmed" checkbox must always be enabled for Connect Plus channels via MOTOTRBO CPS.
However, note that "confirmed" delivery does not imply end-to-end confirmation from the source to the target SU. The confirmation is from the controller to the source SU.

In other digital modes, text messages are always transmitted directly from the source SU to one or more destination SU's. In Connect Plus, text messages are never transmitted directly from one SU to another. They always go through the Connect Plus controller. This means that Connect Plus text message transfer is a two-step process. In the first step, the Source SU requests an available timeslot for text message transmission. The controller assigns a trunk-to timeslot. The Source SU moves to the trunk-to timeslot and transmits the text message to the controller as an IP datagram. The controller receives the text message on behalf of the destination SU, and places the message in the subscriber's mailbox. The controller sends OTA acknowledgement upon receiving the message, and the source SU displays, "Message Sent".
When a timeslot and the Destination ID are both available, the controller initiates the second step in the process, text message delivery, by sending a Control Channel message to assign the trunk-to timeslot. On the trunk-to timeslot, the controller delivers the text message(s) to the Destination ID. When the controller delivers a text message to an individual ID, it expects to receive OTA acknowledgement for each transmitted message. If OTA acknowledgement is not received, the message is re-queued, and the controller re-attempts delivery at a later time. For text messages to a Group ID, the controller does not expect to receive OTA acknowledgement since the message is transmitted in "unconfirmed" mode.

2.6.4 Controller Programming for Text Messaging Services

The XRC controller has several parameters that affect Text Messaging. These are configured with the **MOTOTRBO™ Connect Plus Network Manager**[10] software:

- In order for a radio to receive text messages, the radio must have a display, and the “Text RX Capable Radio” checkbox must be enabled on the SU’s user record in the controller database.

- In order for a radio to send a text message to its Multigroup ID, the “Multigroup Call Init” checkbox must be enabled on the SU’s user record in the controller database. Otherwise, the controller will deny the request.

- In order for a radio to send a text message to the Site All Call Text ID, the “Site All Call Text Init” checkbox must be enabled on the SU’s user record in the controller database. Otherwise, the controller will deny the request

- The next two settings affect Text Message exchange between the Connect Plus setting and a Text Message Server:

    - The Site Configuration screen has a field called, “Text UDP Listen Port”. This setting determines which UDP port the controller utilizes to listen for incoming messages from the Text Message application. Unless it creates UDP port conflict, this should be left at the default setting of UDP Port 4007.

    - The XRC can be configured with a Destination IP address and Port for the Text Message Server. This is only necessary when there are multiple Connect Plus sites, but all sites do not share the same (IP address) perspective back to the TMS server. Otherwise, the controller can use the Server IP address and port that was provided in a special message sent by the Text Message Server.

---

[10] For brevity, the **MOTOTRBO™ Connect Plus Network Manager** will be referred to simply as **Network Manager** from here on.

2.6.5 SU Programming for Text Message Services

The System Design Section has a thorough discussion of how a Connect Plus radio should be programmed with MOTOTRBO CPS. The following section discusses how specific MOTOTRBO CPS settings affect text message operation on Connect Plus channels:

- The Connect Plus **Radio ID** is set with MOTOTRBO CPS. Select a Radio ID between 1 and 16776351 that has not been used for any other radio in the Connect Plus network. This is used as the Source ID for text messages created by this Connect Plus SU and as the Destination ID for text messages created by other SU's and destined for this radio.

- Connect Plus requires that the **CAI Network** and **CAI Group Network** settings must be left at the default values.

- In order for the radio to transmit a maximum size text message plus overhead, the **Max TX PDU** size should be 750 bytes or larger to accommodate a text message of up to 280 Unicode characters.

- **TX Preamble Duration** determines the length of the preamble that is sent before all text messages, regardless of digital mode. This value should be set to **zero**.

- For Connect Plus digital channels, **Compressed UDP Data Header** should be disabled (unchecked).

- For Connect Plus Channels, **Data Call Confirmed** should be enabled (checked).

The following MOTOTRBO settings affect Text Message operation when the radio is selected to non-Connect Plus digital channels, but they are not used by Connect Plus. If the Connect Plus radio is also used for non-Connect Plus digital operation (Digital Conventional, IP Site Connect, Capacity Plus), the MOTOTRBO parameters immediately below should be set according to the requirements of those operations. They have no affect on Connect Plus Operation:

- Pre-programmed (quick text) messages that are programmed with MOTOTRBO CPS.

- TMS Radio ID

- TMS UDP Port

- Forward to PC checkbox

- Digital Contacts created with MOTOTRBO CPS

The following settings in Connect Plus CPS affect text messages

- Create Digital Contacts to represent other radios that this SU may send a text message to, or receive a text message from. Failure to create a digital contact will not keep a display radio, provisioned for Manual Dial, from sending messages to SU's that aren't on the Contact list (or receiving messages from SU's that aren't on the Contact list), but the ID information will be displayed by number only, not by alias. The, "Dispatch Call" contact type, is used exclusively for text messages exchanged between the SU and Text Message Dispatch Clients. A Text Message Dispatch Client is a non-radio entity, such as a Text Message Dispatcher PC.

- Use the Text Messages screen to create programmed (quick text) messages, if desired.

- If desired, use the Buttons screen to set a “One Touch Call”, which can be used to send a configured Quick Text message to a specific Destination ID.

2.6.6 Connect Plus Interface to Text Message Application

Just as in other MOTOTRBO digital modes, Connect Plus supports text message transfer between Connect Plus SU’s and non-Connect Plus entities, such as a Text Message Dispatch PC. The text message transfer is facilitated via the controller’s IP connection to a Text Message application, sometimes referred to as the “Text Message Server”. Connect Plus supports the following services for its interface to the Text Message application:

- A Text Message Dispatch Client can send a text message to a Connect Plus SU.
- A Text Message Dispatch Client can send a text message to a Connect Plus Group ID.
- A Text Message Dispatch Client can send a text message to a Connect Plus Multigroup ID.
- A Text Message Dispatch Client can send a text message to the Connect Plus Site All Text ID.
- A Connect Plus SU can send a text message to a TMS Dispatch Client.
- The Connect Plus controller provides mailboxing for text messages, which allows for store and forward.
- The Connect Plus controller provides automatic retries for text messages sent from a Text Message application to individual Connect Plus ID’s, and for text message sent from a Connect Plus SU to a Text Message application.
- The Connect Plus controller sends a “Confirmation of transmission” text message to a Text Message Client when a message is delivered OTA.
- The Connect Plus controller sends an “Undeliverable Notification” text message to a Text Message Client when a message cannot be delivered OTA.

While many of the Connect Plus services to the TMS application are also available in other MOTOTRBO digital modes, the system architecture for providing these services is different in Connect Plus.

In other digital modes, the Text Message application resides on a PC that has a USB connection to a mobile radio. The control station radio acts as peer to other subscriber units in the field via the Common Air Interface. Connect Plus does not use this architecture. In Connect Plus, the Text Message application resides on a PC that is connected via IP to a XRC Controller. This can be any Connect Plus controller on the radio network. The controller is the application’s gateway to the Common Air Interface. This architecture provides several significant advantages:

- The controller supplies immediate acknowledgement upon receiving the text message via IP. The Text Message application is not responsible for the possible complications of over-the-air delivery. The controller – not the Text Message application – manages over-the-air retries for confirmed text messages.
- By sending the message to the Connect Plus controller, the application is handing it to the central intelligence of the Connect Plus system. The controller is the system component with the required knowledge to locate the destination SU, identify an available RF resource, and deliver the message to its intended target.

- The application can send the text message to any controller at any time. It does not need to worry about where the Destination SU is currently registered, whether the destination SU is currently busy or idle, whether there is a channel currently available for text message transmission, etc. Upon receiving the text message, the controller places the message in the mailbox of the destination SU, and will deliver the message at the earliest opportunity.

- When the controller delivers a text message from a Text Message Dispatch Client to an individual Connect Plus ID, the controller expects to receive OTA acknowledgement that the message has been received from the destination SU. Upon receiving this acknowledgement, the controller sends a "confirmation of transmission" text message to the Text Message Dispatch Client. Or, if transmission cannot be completed successfully, the source Dispatch Client receives an "undeliverable" notification.

- The Motorola Multi-Channel Device Driver (MCDD) is not required, nor used in Connect Plus.

Just as in other digital modes, the "Dispatch Call" Contact type is used to facilitate Text Message exchange between an SU and a TMS Dispatch Client. To illustrate how the Connect Plus system uses this contact type, the following steps are provided:

1. The Connect Plus radio is programmed (via Connect Plus CPS) with one or more "Dispatch Call" entries in its Contact List. When creating the contact, a "Call ID" must be entered for the record (1-16776351). An alias (such as "Central Dispatch", for example) may be entered as well.

2. The Connect Plus user follows the normal procedure to create a text message (or use a programmed "quick text message") and selects a target ID from the Contact List. The Dispatch Call ID ("Central Dispatch, for example) is available as a target. The radio user presses OK.

3. The Source radio requests a timeslot for text message transmission and sends the text message to the controller. The controller knows through a couple of different mechanisms that message is destined for a TMS Dispatch Client. However, the message itself does not include the IP address of the TMS Server, or the TMS Dispatch Client.

4. The controller looks up the Destination IP address and port number for the Text Message Server, and forwards the message accordingly via its IP connection. There are two different ways the controller can determine the Text Message Sever IP.

   a. The Text Message server can send a special message to the controller called the "Text Message Service Availability Message". The message targets a specific SU, and it provides the IP address of the Text Message Server. Upon receiving the message, the controller stores this information on behalf of the targeted SU. When the SU sends a message to the Text Message Server, the controller can use this stored IP address when forwarding the text message to the Text Message Server. This approach allows different SU's to have different Text Message Servers, but it cannot be used in a multisite network when different sites have a different (IP address) perspective back to the TMS Server. In that case, the controller must use a programmed IP address for the Text Message Server as discussed in the next paragraph. Which approach is actually used (Service Availability Message or programmed Text Message Service IP address) is determined through controller programming.

   b. The XRC controller can be programmed with a Destination IP address and port for the Text Message Server. Because this is a site-wide setting (which means that the controller will use the same Text Message Server IP for all SU's), programming the Text Message Server IP address into the controller provides somewhat less flexibility than obtaining this address from the Service Availability Message. This approach is required in a multisite network when different sites have a different (IP address) perspective back to the TMS Server. Regardless of which approach is used, it should be noted that Connect Plus does not support multiple Text Message Servers for messages sourced by the same SU.

5. The server receives the text message and decodes the “Dispatch Call ID” that was selected by the radio user. The server has a lookup table to translate the Call ID to a user name, destination IP address and port. This tells the Text Message server how to route the message to the destination Dispatch Client. If supported by the Text Message Server, the Dispatch Call ID can be translated into an email address; thereby providing a text message interface between Connect Plus SU’s and email clients. It should be noted that all text messages exchanged with the Connect Plus system have a maximum length of 280 characters, which is the same as other MOTOTRBO digital modes.

When a Text Message Dispatch Client sends a Text Message to a Connect Plus SU, the process described above is followed in reverse. In order to receive a text message from a Dispatch Client, the SU doesn’t necessarily have to be programmed with the Dispatch Call ID used by the Text Message server, but this is highly recommended. It is required in order to display a programmed alias, and it is also required for the SU to source a text message to the Dispatch Client (unless the SU is replying to a previously received message).

Note: As a general rule, information sent from a data application (such as a Text Message application) to the XRC controller is not stored to persistent memory. Such information can sometimes be lost if a controller resets, or if there is a redundant controller “failover”. This depends on many factors such as which site reset (or experienced failover), what type of information was sent, where the destination SU was registered at the time, etc. The recommendation to the Network Administrator is as follows: If you become aware that a XRC (anywhere in the network) has reset or experienced redundant controller “failover”, stop (close) the data application, and then restart the application. This will cause the data application, following start-up, to resend critical messages and requests to the Connect Plus network.

2.6.7 Text Message Size

In Connect Plus, all text messages pass through the XRC Controller prior to delivery to their final destination. This allows the controller to truncate the message length prior to delivery, if necessary. The maximum text message size (length) depends on the Connect Please Release software version:

- Prior to System Release 1.7 (R2.6.0), the maximum supported text message size was 140 characters. If the XRC Controller received a text message of greater than 140 characters, it truncated the text message to 140 characters prior to delivery. This remains the expected operation of any Controller with firmware prior to Release 1.7 (R2.6.0).

- Beginning with System Release 1.7 (R2.6.0), the maximum text message size supported by the controller is 280 characters. The controller operation for truncating text messages, if necessary, is discussed later in this section. The maximum text message size supported by the Connect Plus radio is as follows:

    - 280 characters for received text messages.
    - 278 characters for text messages created from the radio’s keypad.
    - 138 characters for quick text messages created from MOTOTRBO Connect Plus CPS configuration.

Note: The Connect Plus radio supports text messages of greater than 140 characters when (a) the radio’s Option Board firmware supports extended text messages, and (b) when “Extended Text Messages” appears on the Device Features screen after reading the radio with MOTOTRBO CPS.

Controller operation for truncating text messages

Beginning with Release 1.7 (R2.6.0), the controller operation for truncating text message length depends on whether the text message is targeted to a Private ID or to a Group ID.

- Private Text Messages:
    - If a private text message of greater than 140 characters targets a radio with Option Board firmware that does not support extended text messages, the controller truncates the message to 140 characters prior to attempting delivery. The text message source (which can be a radio or text message application) is not informed of the truncation, but the controller creates a time-stamped Event Log entry.
    - If a private text message of greater than 140 characters targets a radio with Option Board firmware that supports extended text messages, the controller transmits the entire text message (up to 280 characters).
- Group Text Messages:
    - The controller truncates any Group text message of greater than 280 characters to 280 characters prior to transmitting the message. (Text Message applications should not create any text message of greater than 280 characters.)
    - The controller does not truncate any Group text message to 140 characters as it does with some Private Text Messages.

Connect Plus Radio Operation Upon Receiving Group Text Messages

- If the receiving radio does not have Connect Plus Option Board firmware that supports extended text messages, and if the radio receives a Group text message of greater than 140 characters, it will not display the received message at all. Neither will it provide any indication of having received the message.
- If the receiving radio has Connect Plus Option Board firmware that supports extended text messages, and if “Extended Text Messages” appears on the MOTOTRBO CPS Device features screen, it will display up to 280 characters of a received text message (after selecting the message from the Inbox).

2.6.8 Text Messaging Features not Available in Connect Plus

The following Text Message features are not available in Connect Plus:

- In other digital modes, Text Messages to an individual SU can be sent either confirmed (acknowledgement requested) or unconfirmed (no acknowledgement requested). This is a programmable option with MOTOTRBO CPS. In Connect Plus, all Text Messages to an individual SU must be transmitted in confirmed mode. This means that the “Data Call Confirmed” checkbox must enabled for all Connect Plus personalities when programming the radio with Connect Plus CPS.
- In other digital modes, the SU can be configured so that it will forward text messages received OTA to a connected PC. This option is not available for Connect Plus operation.
- In other digital modes, the radio will transmit text messages that were received from a directly connected PC. This is not available for Connect Plus operation.

2.7 Connect Plus Location Services

Connect Plus Location Services support “single” and “periodic” Location Updates for GNSS-equipped SU’s (outdoor location tracking) and for Bluetooth-equipped SU’s (indoor location tracking).

Outdoor location tracking, utilizing the radio’s GNSS/GPS receiver, has been supported the initial Connect Plus System Release. Starting with System Release 1.7 (R2.6.0), Connect Plus also supports the ability to report iBeacons signals detected by the radio’s Bluetooth receiver. This technology can be used to track a radio’s location in places where satellite GNSS/GPS signals cannot normally penetrate. For more information on Indoor Location Reporting, see section “*Connect Plus Indoor Location Tracking*”.

Just as in other digital modes, Connect Plus updates are initiated at the request of a Location Server by utilizing the Location Request Response Protocol (LRRP). The location server can request the radio to send GNSS/GPS data (outdoor location), beacon data (indoor location), or both types of data in a single report, depending on the radio’s hardware and software capability. The information in the following sub-sections, including Fast GPS, applies to both outdoor and indoor location updates, unless otherwise noted. The LRRP system architecture for Connect Plus is different from other digital modes. The Connect Plus architecture is illustrated and discussed in following diagram and text.

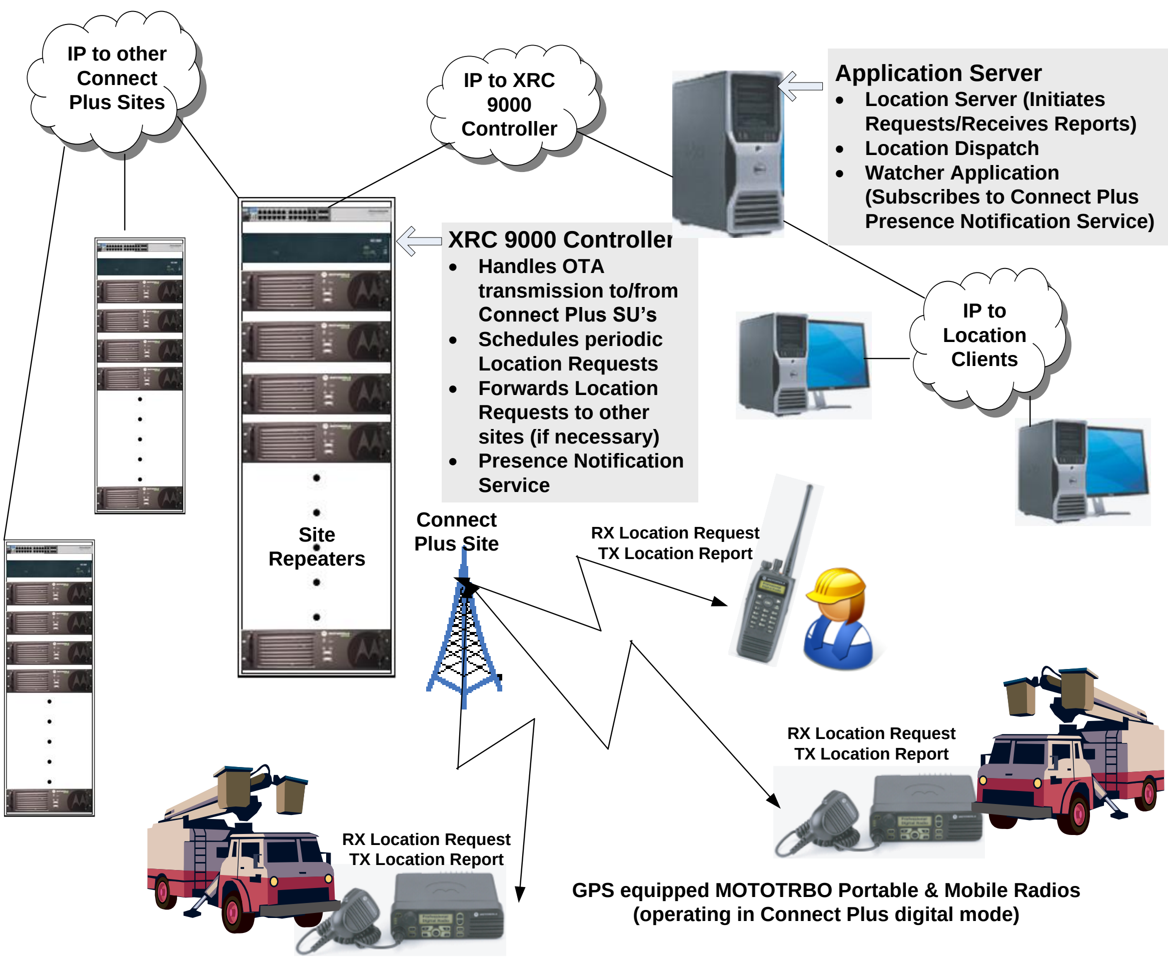


Figure 2-5 Connect Plus Location Services

In Connect Plus, the Location application resides on a PC that is connected via IP to a XRC Controller. This can be any Connect Plus controller on the radio network. The controller is the application’s gateway to the Common

Air Interface. Figure 2-5 shows the described Location Service configuration. This architecture provides several significant advantages:

- By sending the Location Request to the Connect Plus controller, the application is handing it to the central intelligence of the Connect Plus system. The controller is the system component with the required knowledge to locate the destination SU, identify an available RF resource, and send the Location Request to its intended target. The application does not need to worry about the destination SU is currently busy or idle, whether there is a channel currently available for Location request transmission, etc. Upon receiving the Location Request, the controller will transmit the Request to the destination SU at the earliest opportunity.

- Because the controller assigns which timeslot will be used for Location Requests and Reports, it can utilize any available timeslot for location updates not obtained via the Fast GPS method. For periodic location updates obtained via the Fast GPS method, the controller utilizes a Fast GPS Report Channel. For more information on Fast GPS, see the section called, “Connect Plus Fast GPS”.

- In other digital modes, the SU runs a timer to track its “periodic interval”, and transmits its Location update to the “Selected Channel” or its “GPS Revert Channel” (depending on CPS programming) when the timer expires. This approach is susceptible to collisions that occur when two or more SU’s pick the same time and channel to transmit their location update. In Connect Plus, the controller tracks both the periodic interval and assigns the timeslot for the Location Update. This allows the Connect Plus system manage resource assignment in an orderly manner, and to provide a collision-free environment for periodic Location updates.

- The Multi-Channel Device Driver (MCDD)[11] is not required for the Location Server when interfacing to the Connect Plus network. The application sends the request to any XRC controller in the network. The application does not need to be concerned about what site or channel the SU is currently using. Tracking the SU between sites is the responsibility of the controller. The Location Report might not come from the same controller that received the Location Request.

Note: As a general rule, information sent from a data application (such as a Location Services application) to the XRC controller is not stored to persistent memory. Such information can sometimes be lost if a controller resets, or if there is a redundant controller “failover”. This depends on many factors such as which site reset (or experienced failover), what type of information was sent, where the destination SU was registered at the time, etc. The recommendation to the Network Administrator is as follows: If you become aware that a XRC (anywhere in the network) has reset or experienced redundant controller “failover”, stop (close) the data application, and then restart the application. This will cause the data application, following start-up, to resend critical messages and requests to the Connect Plus network.

2.7.1 Single Location Update

When the XRC controller receives a Single Location Update request for a registered SU, the operation is as follows:

- The controller forwards the request to the registered site (if different from the site receiving the request).

- The controller of the registered site checks SU and timeslot availability. At the earliest opportunity, it sends a Control Channel message to move the destination SU to a trunk-to timeslot.

- On the trunk-to timeslot, the controller transmits the Location Request, using confirmed or unconfirmed data transfer (depending on the configuration of the SU record in the controller database).

[11] The reader can refer to the MOTOTRBO System Planner regarding the Multi-Channel Device Driver.

- On the same trunk-to timeslot (during the same session), the SU transmits its Location Report, also using confirmed (or unconfirmed) data transfer (depending on the configuration of the SU record in the controller database).

- The controller forwards the Location report to the requesting Location application.

- After completing the process, the controller deletes the Request and its corresponding Report.

2.7.2

2.7.3 Periodic Location Update

This section describes the original Connect Plus method for sending Periodic Location Updates on a regular voice/data traffic channel via confirmed datagram transmissions. For information on Connect Plus Fast GPS, which supports higher throughput for Periodic Location Updates by sending unconfirmed data transmissions on a dedicated GPS channel, see section, "Connect Plus Fast GPS".

When the XRC controller receives a Periodic Location Request (also called a "Triggered Request with Periodic Interval") for a registered SU, the operation is as follows:

- The controller sends a message to the requesting application verifying receipt of the periodic Location Request.

- The controller forwards the request to the registered site (if different from the site receiving the request).

- The controller converts the request to a Single Location Request, making note of the requested periodic interval.

- The controller of the registered site checks SU and timeslot availability. At the earliest opportunity, it sends a Control Channel message to move the destination SU to a trunk-to timeslot. The controller tells the SU that it should store the imminent Location Request.

- On the trunk-to timeslot, the controller transmits the Location Request, using confirmed or unconfirmed data transfer (depending on the configuration of the SU record in the controller database).

- On the same trunk-to timeslot (during the same session), the SU transmits its Location Report, also using confirmed (or unconfirmed) data transfer.

- The controller converts the Single Location Report to a Periodic Location Report (to match the original request), and forwards the Location report to the requesting Location application.

- The controller tracks the requested periodic interval. When the requested interval expires, the controller of the registered site checks SU and timeslot availability. At the earliest opportunity, it sends a Control Channel message to move the destination SU to a trunk-to timeslot. The controller tells the SU that it should use its stored Location Request. This speeds up the data transfer on the trunk-to timeslot.

- On the assigned trunk-to timeslot the SU transmits a Location Report based on its stored Location Request. It is important to point out that the combined duration for Location Request from the controller and the corresponding Location Report from the SU is about 2-3 seconds (assuming no retries). After receiving the Location Report the controller resets the timer for the periodic interval for the given SU. The net effect of this approach is that the actual periodic interval is increased by 2-3 seconds.

- The controller converts the Single Location to a Periodic Location Report (to match the original request), and forwards the Location report to the requesting Location application.

- The process described above is repeated at each periodic interval until in one of the following occurs:
  - The requesting Location application cancels the periodic request, or
  - The requesting application sends a new periodic request, or
  - The request times out. To prevent the request from timing out, the application must resend the request prior to expiration of the controller's Location Request Time Out (24 hours).
  - The SU de-registers from the network

The Connect Plus system supports just one periodic request at a time for any SU (and therefore just one requesting application at a time for any SU). The radio's periodic location report can contain GNSS/GPS (outdoor) location data only, beacon (indoor) location data only, or both types of data in the same periodic report, depending on radio capability and the LRRP elements requested by the location application.

2.7.4 Sending Reports to the Location Application

When the XRC controller sends the Location Report to the requesting application, there are two different ways the controller can determine what IP address and port it should use for the Location application:

- Upon receiving a Location Request from a Location application, the controller stores the Source IP and Port from the received request. When the SU sends the Location Report to the XRC, the controller can use this stored IP address when forwarding the report to the requesting application. This approach provides the most flexibility. Because the controller uses the IP address stored from the request, multiple Location servers can request a single location update from same SU (but just one a time). For periodic updates, this approach allows different SU's to have different Location Servers (but all periodic updates for the same SU will be sent to the same Location Server). This approach (using the IP address stored with the request) cannot be used in a multisite network when different sites have a different (IP address) perspective back to the LRRP Server. In that case, the controller must use a programmed IP address for the Location Server as discussed in the next paragraph. Which approach is actually used (using the IP address from the request or using a programmed Location Server IP address) is determined through controller programming.

- The XRC controller can be programmed with a Destination IP address and port for the Location Server. Pre-configuring the Location Server IP address into the controller provides somewhat less flexibility than obtaining this information from the received request. Because this is a site-wide setting, all location reports (both "single" and "periodic" reports), for all SU's, go back to the same Location Server. This approach is required in a multisite network when different sites have a different (IP address) perspective back to the LRRP Server.

2.7.5 Location Services and Presence Notification

The Connect Plus system does not retain any type of Location Request when the destination Connect Plus SU de-registers from the network. Also, if the controller receives a Location Request for an un-registered SU, it does not store the request. The Location application must send the request while the SU is registered with the network. For these reasons, it is highly recommended that Location application take advantage of the controller's Presence Notification services. By implementing this interface, the Location application can send the Location Request when it receives a message from the controller (acting as Presence Notifier) which indicates that the SU is "present" in the network. For more information, see "Connect Plus Presence Notifier" section.

2.7.6 Controller Programming for Location Services

The XRC controller has several parameters that affect Location Services. These are configured with the MOTOTRBO Connect Plus Network Manager software:

- In order for a radio to respond to Connect Plus location requests, the radio must be GNSS-equipped, and the "GPS capable radio" checkbox must be checked on the SU's user record in the controller database, or the radio must be Bluetooth-equipped, and the "Indoor Location Reporting Capable" checkbox must be checked on the SU's user record in the controller database. If the radio supports and sends both GPS and indoor location data, then both boxes must be checked. There are two additional location-related flags per user record; "Enable Unconfirmed LRRP" and "Enable Fast GPS". For more information on the operation of these flags, see the table below.

- The Site Configuration screen has a field called, "LRRP UPD Listen Port". This setting determines which UDP port the controller utilizes to listen for incoming Location requests from the Location application. Unless it creates UDP port conflict, this should be left at the default setting of UDP Port 4001.

- The XRC can be configured with a Destination IP address and Port for the Location Server. This is only necessary when there are multiple Connect Plus sites, but all sites do not share the same (IP address) perspective back to the LRRP server. Otherwise, the controller can use the Server IP address and port that was provided in the location request.

- If the Connect Plus site supports Fast GPS Report Channels, there are several configurable settings that help determine how the controller uses and assigns the report channels. For more information on these settings, see section, "Connect Plus Fast GPS". Detailed configuration information is also available in the XRC Controller User Guide and MOTOTRBO Connect Plus Network Manager Help File.

  There are four configurable flags per SU record in the Connect Plus user database that help determine GPS/LRRP operation. The flags are "GPS Capable", "Indoor Location Reporting Capable", "Enable Unconfirmed LRRP" and "Enable Fast GPS". The table below shows how these flags determine GPS/LRRP operation.

GPS Capable and Indoor Location Reporting Capable checkboxes	Enable Unconfirmed LRRP checkbox	Enable Fast GPS[12] checkbox	How the session is assigned	How report is sent
both unchecked	unchecked	unchecked	N/A (no GPS)	N/A (no GPS)
either/both checked	unchecked	unchecked	For all types of location sessions, the Control Channel sends a SUID-specific assignment message for each session.	For all types of location reports, the radio uses confirmed data transmission on a regular traffic channel.
either/both checked	**checked**	unchecked	For all types of location sessions, the Control Channel sends a SUID-specific assignment message for each session.	For all types of location reports, the radio uses unconfirmed data transmission on a regular traffic channel.
either/both checked	**checked**	**checked**	For Periodic Location reports: Control Channel sends window/frame announcements. A single announcement message can trigger reports from multiple radios. For other types of LRRP sessions: Control Channel sends a SUID-specific assignment message for each session.	For Periodic Location Reports: The radio uses unconfirmed data transmission on a dedicated Fast GPS Report channel. For other types of LRRP sessions: The radio uses Unconfirmed data transmission on a regular traffic channel.

Table 2-2 GPS Options in Network Manager

2.7.7 SU Programming for Location Services

The System Design Section has a thorough discussion of how a Connect Plus radio should be programmed with MOTOTRBO CPS. The following section discusses how specific MOTOTRBO CPS Settings affect Location Services for the Connect Plus SU:

- For a GPS equipped radio, the "GPS" checkbox must be enabled on the General Settings screen with MOTOTRBO CPS. This enables the GPS receiver and causes a display radio to show the GPS icon. In Connect Plus mode, the GPS icon is visible while the Option Board is idle and monitoring the control channel. The icon is not shown during a call-in-progress.
    - The absence of this icon indicates that the location service is disabled.
    - The icon shows a full satellite dish when good GPS signals are detected.

[12] Fast GPS requires the site to be authorized for one or more Fast GPS Report Channels. For more information on Connect Plus Fast GPS, see the section called, "Connect Plus Fast GPS".

  - The icon shows an empty satellite dish when the radio is receiving poor GPS signals. If the SU has previously acquired the satellite, and then lost it, it may transmit its last known location even though the GPS coordinates may no longer be valid.

- The Connect Plus **Radio ID** is set with MOTOTRBO CPS. Select a Radio ID between 1 and 16776351 that has not been used for any other radio in the Connect Plus network. This ID must be configured into the Location server, along with the requested attributes (location, velocity, etc.) The Radio ID is used as the Destination ID for Location Requests sent to this Connect Plus SU, and it is used as the Source ID for Location reports received from this SU.

- Connect Plus requires that the **CAI Network** and **CAI Group Network** settings must be left at the default values.

- The **Max TX PDU** must be large enough to accommodate the largest Location Report expected from this SU. Recommended value is 500 bytes or larger. Set to 1500 bytes to accommodate maximum possible location report size containing indoor location elements.

- **TX Preamble Duration** determines the length of the preamble that is sent before the IP datagram containing the SU's Location Report. This value should be set to **zero**.

- For Connect Plus digital channels, set "Compressed UDP Header" to "None". This will not prevent the Connect Plus radio from utilizing the Compressed UDP Data Header when the XRC Controller expects it do so.

- For Connect Plus Channels, **Data Call Confirmed** should be enabled (checked). This will not prevent the Connect Plus radio from making unconfirmed data calls when the XRC Controller expects it do so.

- MOTOTRBO CPS displays the Indoor Location screen, depending on radio model, firmware level, and device features. It is used to enable Indoor Location tracking, to configure the beacon scan timers, and to create a list of Beacon UUIDs the radio will respond to. For more information, see section "Connect Plus Indoor Location Tracking".

Due to the Connect Plus Option Board's role in providing Location services, there are some MOTOTRBO CPS Location parameters that affect non-Connect Plus personalities only. The settings listed below are important for configuring Location updates in other digital modes, but they have no effect on Connect Plus operation:

- The **Persistent LRRP Requests "Save"** checkbox does not affect Connect Plus operation.

- **The Persistent LRRP Requests "Delete"** checkbox does not affect Connect Plus operation.

- **ARS** checkbox. ARS is not used in not used in Connect Plus. This checkbox is grayed out when "Option Board Trunking" is enabled for the digital personality.

- **GPS Revert** field. Connect Plus does not use a GPS Revert Channel. Because this setting is tied to the ARS Checkbox, it will be grayed out when "Option Board Trunking" is enabled for the digital personality.

The following Connect Plus CPS Settings affect Location Services for the Connect Plus SU:

- At the present time, there are no programmable settings in Connect Plus CPS specifically for Location Services.

2.7.8 Connect Plus GPS Performance Specifications

The Connect Plus is subject to the same performance specifications as other MOTOTRBO digital modes in regards to the following:

- Cold Start
- Hot Start
- Time to First Fix (TTFF)
- Horizontal Accuracy

For more information on these topics, see "Performance Specifications" in *Location Services* section of [1].

2.7.9 Location Report Rates in Connect Plus

Because all Location requests go through the controller in Connect Plus trunking, this additional step will add some additional time for the Location Request-Report process when compared to the best-case scenario for other digital modes. The trade-off is that Connect Plus virtually eliminates collisions for Location Requests and Reports and provides a highly managed environment for channel assignments. Even so, it should be noted that the controller will process all requests on a best effort basis that will be influenced by factors such as channel availability, the number of other calls in process (both voice and data), and the number of requests being processed. Immediate Requests may not always receive an Immediate Report. Periodic reports may not always come at the exact, requested interval. On a "quiet" Connect Plus site, the controller can use every trunk-to timeslot for Location Updates, resulting in a very high update rate. The rate will decline as requests for other types of calls increase.

The Connect Plus Fast GPS (Fast GPS) feature was introduced in Connect Plus System Release 1.6. Fast GPS provides higher throughput for location updates by providing one or more dedicated Fast GPS Report Channels per site that are not shared with other types of calls. This allows location reports to continue, even when the site does not have any available resources for voice or other types of data calls. For more information, see section "Connect Plus Fast GPS".

2.7.10 Emergency Location Update

Connect Plus supports Emergency Location Update, a special type of "Triggered Location Request".

In Connect Plus, the 3rd party Location Application sends the Triggered Request for Emergency to any of network's XRC controllers when an "SU of interest" registers into the network. (If the 3rd party Location Application has subscribed to the XRC's "Presence Notification" services, it will be notified when the SU of interest registers or de-registers with the Connect Plus network.)

The XRC will acknowledge the Emergency Location Request on behalf of the Destination SU, and then store the request for the SU until it is needed.

Whenever the XRC receives an Emergency Call Request from an SU, the controller checks to see if a 3rd party LRRP application has requested an Emergency Location Update for this SU. If so, the XRC takes the following actions:

- Upon decoding an Emergency Alert or a Call Request CSBK for an Emergency Call, the XRC sends a message to the LRRP application that an emergency condition has been detected for an SU of interest. This message does not contain the SU's location information. The Emergency Alert session or the Emergency voice call must conclude prior to the Emergency Location Update. The XRC sends this message one time for each Emergency Alert or Emergency Call request that it decodes from the SU of interest. It is up to the receiving application as to how it processes this message (if at all).

- In its response to the SU initiating the emergency, the Controller informs the SU that an Emergency Location Update should occur at the end of the Emergency Alert or Emergency voice call.

When the Emergency Alert or Emergency call is over, the SU sends a message to XRC controller requesting a trunk-to timeslot for the Emergency Location Update. The controller assigns a times slot for the Emergency Location Update, or places the request in the Busy Queue if none is available. When assigning calls from the Busy Queue, only Emergency Calls (emergency voice) have precedence over Emergency Location Updates (emergency data).

After assigning a trunk-to timeslot for the Emergency Location Update (which may or may not be the same timeslot used for the Emergency Call), the controller transmits the stored Triggered Location Request (Emergency) to the Destination SU. The Connect Plus SU responds by sending the requested information. Upon receiving the Emergency Location Update, the controller forwards the report to the requesting application.

If the Emergency Location Update session fails on the trunk-to timeslot, the controller will not have a report to send to the 3rd party application. As a courtesy to the Location application, the controller sends a blank Triggered Location Report on behalf of the destination SU. Upon receiving this report, the LRRP application can send an Immediate Location Request for the destination SU, if so desired.

Another situation when the Emergency Location Update may not convey the real location of the emergency initiator is in the case when the SU does not have a GNSS/GPS lock during the emergency event. In this scenario the Emergency Location Update received by the controller will contain stale GNSS/GPS coordinates, but will be forwarded to the 3rd party application as it is. The LRRP application needs to evaluate the Location Report "quality" and decide how to present the information to the user.

The Connect Plus system supports just one emergency location request at a time for any SU. The radio's emergency location report can contain GNSS/GPS location data only, beacon location data only, or both types of data in the same report, depending on radio capability and the LRRP elements requested by the location application.

2.7.11 Confirmed vs. Unconfirmed Location Reports

In Connect Plus operation, the radio MOTOTRBO CPS codeplug should always be configured for confirmed data enabled. However, this does not prevent the Connect Plus radio from transmitting unconfirmed data when the XRC Controller expects the radio to do so.

In confirmed data operation, the source device expects over-the-air acknowledgement that that the target device has received its data transmission. If no such acknowledgement is received with an expected time frame, the source device makes up to three total transmission attempts, applying a wait time after each attempt. The main benefit of confirmed data is that the source device usually knows whether the target has received its data. (It is possible that the target received the data, but the source didn't receive the confirmation.) Confirmed data transmission for location requests and reports continue to be supported and utilized when the "Enable Unconfirmed LRRP Reports" box is **not** checked on the target radio's unit record in the Connect Plus subscriber database.

Connect Plus also supports unconfirmed data transmissions for location requests and reports. Unconfirmed data utilizes a single, unconfirmed UDP/IP datagram for each request or report, whereas confirmed operation varies from 1 to 3 datagram transmissions, depending on when (and if) confirmation is received. Therefore, the average traffic channel session is much shorter when using the unconfirmed data method. This results in a higher throughput (more reports per minute) per channel than the confirmed data method.

Even though the unconfirmed method does not require (or expect) confirmation of receipt, its reliability is as good as, or better than, the confirmed data method for *small* data payloads. This is because the unconfirmed method allocates more bits to Forward Error Correction. In addition, all Connect Plus unconfirmed location reports utilize UDP/IP header compression. This results in a further speed improvement over the Connect Plus confirmed method, which utilizes the standard (non-compressed) UDP/IP Header[13].

Connect Plus uses the unconfirmed data method for location requests and reports when the "Enable Unconfirmed LRRP Reports" box is checked on the target radio's unit record in the Connect Plus subscriber database.

2.7.12 Connect Plus Fast GPS

Connect Plus Fast GPS provides several improvements over the original (non-Fast GPS) Connect Plus method for sending periodic location reports:

1. Connect Plus Fast GPS uses Control Channel messaging and bandwidth more efficiently. In the original method, the controller sends a SUID-specific Control Channel assignment message for each report session. This assignment method is still used for all non-Fast GPS location report sessions. The Control Channel bandwidth that is available to assign non-Fast GPS location reports varies depending on site activity, and can affect report throughput.

   Whereas the original method requires a Control Channel assignment message for each location report session, Fast GPS assigns anywhere from 1 to 56 Fast GPS periodic reports with a single Control Channel message. The range varies so widely because it depends on (a) how many Fast GPS Report Channels the site is currently using and (b) how heavily loaded each Fast GPS Report Channel currently is.

2. In Fast GPS, periodic location reports are sent on a dedicated Connect Plus Fast GPS Report Channel. In this way, Connect Plus Fast GPS assures an RF resource for periodic location reports, thereby

[13] In the radio MOTOTRBO CPS codeplug, for each Connect Plus digital channel, set "Compressed UDP Header" to "None". This will not prevent the radio from utilizing the MSI Compressed UDP Header when the controller is expecting it.

allowing location reports to continue at a predictable rate, even while the non-Fast GPS traffic channels are busy with voice and/or other types of data.

3. Fast GPS requires less airtime for each location report than the original method. This is because Fast GPS utilizes a single, unconfirmed datagram transmission for each subsequent update, whereas the original method uses the confirmed method, which varies from 1 to 3 datagram transmissions, depending on when (and if) confirmation is received. Therefore, the average traffic channel session is shorter in Fast GPS than in the original method. Because of this, each report channel supports a higher throughput (more reports per minute) than the original method.

   It should be noted that even subscriber radios that are not enabled for Fast GPS can send unconfirmed location reports. If the radio is enabled for unconfirmed LRRP, but not for Fast GPS, then the location reports are sent on a regular traffic channel, subject to resource availability. In this case, the number of location reports that can be sent on a regular traffic channel is greater than when confirmed data is used, but the overall system throughput is still dependent on the number of Control Channel messages that are available to assign the traffic channel sessions. Fast GPS is required to maximize overall system throughput for location reports.

4. The unconfirmed datagram transmission method, which is utilized by Fast GPS, dedicates more bits to Forward Error Correction than confirmed datagram transmission.

5. All Connect Plus unconfirmed location reports utilize Motorola Solutions Inc. (MSI) UDP/IP header compression. This results in a further speed improvement over the original method which utilizes the standard (non-compressed) UDP/IP Header.

Notes:

- The radio's Fast GPS location report can contain GNSS/GPS (outdoor) location data only, beacon (indoor) location data only, or both types of data in the same report, depending on radio capability and the LRRP elements requested by the location application.
- The original (non-Fast GPS) method of sending periodic location reports continues to be supported. The method that is used (Fast GPS or non-Fast GPS) is configurable per subscriber user record. See section "Controller Programming for Location Services", for more information.

<u>Fast GPS Report Channel</u>

A key element of Connect Plus Fast GPS is the Fast GPS Report Channel.

The Fast GPS Report Channel is a repeater timeslot that is dedicated to receiving periodic location reports from subscriber radios. Anytime that subscriber radios are assigned to a Fast GPS report channel, it will only be used for periodic location reports. It will not be used for voice or other types of data. This includes Emergency Calls and Emergency Location updates.

The number of subscriber radios that can send location reports to a single Fast GPS Report Channel depends on various factors such as the report size configured into the Network Manager and the report interval for each SU. The Fast GPS Report Size is the number of bursts that the SU needs to transmit its report. If a site has more radios enabled for Fast GPS than can be handled by a single Fast GPS Report Channel, then additional Fast GPS Report Channels can be added, up to the maximum number of Fast GPS Channels that are authorized for the site. A single site controller supports a maximum of 28 Fast GPS Report Channels.

The Fast GPS-enabled subscriber radios access their Fast GPS Report Channel(s) in a synchronized manner. The synchronization between subscribers is achieved by a special Control Channel announcement message that time-divides the Fast GPS Report Channel report channel uplink into "windows", "frames" and "superframes".

> **Window**: The smallest time division of the Fast GPS Report Channel uplink. In a single window, one radio can transmit one location report. The time allocated for a single window depends on the Report Size

configured in the Network Manager, and varies from under ½ second (for a Report Size of 5) to ¾ second (for a Report Size of 10).

Frame: A time division of the Fast GPS Report Channel uplink. The amount of time required to announce a single frame is determined by (and is the same as) the fastest supported Fast GPS Report Interval. The time to announce one complete frame is approximately 30 seconds. The number of windows per frame depends on the Report Size configured in the Network Manager. The number of windows per 30-second frame varies from 70 (for a report size of 5) to 40 (for a report size of 10).

Superframe: A time division of the Fast GPS Report Channel uplink consisting of sixteen consecutive frames (frame numbers 1-16). The time to announce one complete Fast GPS superframe is approximately 8 minutes.

The windows and frames that comprise a superframe can be thought of like a spreadsheet. In the figure below, the frames are like Columns. There are always 16 frames in a superframe. The windows are like Rows. The number of windows per frame depends on the Report Size configured into the Network Manager.

	Frame															
Window	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1																
2																
3																
4												F12 W4				
5																
6																
...																

Figure 2-6 Fast GPS: Windows and Frames

The number of windows that will be assigned to any single SU during a Fast GPS superframe depends on the periodic report interval for the SU that was requested by the application.

In a single superframe, the controller announces each window number 16 times, but each time the window number is associated with a different frame number. Therefore, every window in a superframe has a specific address, which is the intersection of the frame number and the window number. This specific address can be thought of as a “cell” in the superframe. The figure above shows an example of a specific address (Window 4 within Frame 12). In this single window (or cell), one SU can transmit one location report **per** Report Channel.

Fast GPS Configuration

Connect Plus Fast GPS does not require any special configuration in MOTOTRBO CPS or MOTOTRBO Connect Plus CPS (beyond what is required for normal radio set-up).

There are several configurable Fast GPS-related settings in the controller. These settings are configured with the MOTOTRBO Connect Plus Network Manager.

- For any subscriber radio that will perform Fast GPS, the radio must be enabled for “GPS Capable Radio”, “Unconfirmed LRRP Reports”, and “Fast GPS” under “Call Privileges” on the radio’s unit record in the Connect Plus subscriber database.
- The Network Manger’s Fast GPS tab contains a number of settings that help determine Fast GPS Operation. The majority of these settings are discussed in subsequent sections. For detailed information, please see the MOTOTRBO Connect Plus Network Manager Help File or the XRC Controller User Guide.

It is also important to understand how the customer’s location tracking software impacts Fast GPS operation. For example:

1. The GPS location data that is included in the radio's report is determined by the request sent by the location application. This has a major impact on the radio's report size, and also on Fast GPS Report Channel throughput. These topics are discussed in subsequent sections.

2. The radio's periodic report interval is configured in the location application, and it must be set to one of the values supported by Fast GPS, as discussed in the next section.

The radio's Report Interval on its Fast GPS Report Channel

The radio's Report Interval determines how often the radio transmits a periodic location report on its assigned Fast GPS Report Channel. Connect Plus currently supports Fast GPS report intervals of **30 seconds, 1 minute, 2 minutes, 4 minutes or 8 minutes**. The radio's report interval is configured into the location application software. It is not configured into the Connect Plus controller or Connect Plus CPS.

If a location application requests a periodic update interval that is different from one of these supported values, and if the target SU is enabled for Fast GPS on its SU record, then the request will be denied by the controller. Therefore, it is important to know which radios have been enabled for Fast GPS in the Connect Plus subscriber database prior to scheduling the SU's update interval in the location application.

The number of different radios that can be accommodated on a Fast GPS Report Channel is influenced by the report interval of those radios. This is because anywhere from 1 to 16 windows (or cells) within the same superframe can be assigned to the same radio, depending on its report interval.

The table below shows how many cells will be assigned to the same SU within a single superframe, depending on the radio's Report Interval. When a SU is assigned multiple windows (or cells) within a superframe, those windows will have the same window number, but a different frame number.

SU Report Interval	Number of "cells" assigned to SU in the superframe
8 minutes	1
4 minutes	2
2 minutes	4
1 minute	8
30 seconds	16

Table 2-3 Total Windows (cells) per Superframe for Single SU, by Report Interval

Table 2-3 helps illustrate how the number of different radios assigned to the same Fast GPS Report Channel depends largely on the report interval for those radios. If every radio assigned to the channel reports once every 8 minutes, then the channel supports 16 times as many different radios as when all assigned radios have a 30-second interval. It is not necessary for all radios to have the same report interval, since the controller can assign radios with different report intervals to the same Fast GPS Report Channel.

Planning for the correct number of Fast GPS Report Channels per site

One of the most important decisions that the system owner or administrator must make is to determine how many Fast GPS Report Channels should be authorized and enabled for each Connect Plus site.

A XRC Controller can be authorized for a specific number of Fast GPS Report Channels at time of purchase (or after the controller has already been deployed to the field). If there is a Primary Controller and a Secondary Controller at the site (to support Redundant Controller Failover), then each controller must be authorized for the same number of Fast GPS channels in order to continue using the Fast GPS feature after failover. For information on how to obtain Fast GPS Report Channel licenses (or how to obtain additional licenses), contact your Motorola Solutions sales representative.

The number of Fast GPS Report Channel timeslots that are currently enabled (authorized) in the controller is displayed on the Network Manager's Fast GPS tab and on the Feature Status screen. It should be noted that the repeater feature called "Enhanced GPS" (viewable via the MOTOTRBO CPS Device Features screen), is not required for the repeater to be used with Connect Plus Fast GPS.

To determine how many Fast GPS Report Channels are required per site, the radio System Administrator must understand all of the following about the Fast GPS-enabled radios on the site/network.

1. What is the largest Report Size (in bursts) that will be transmitted by any Fast GPS radio? This determines the Report Size that will be configured into the Network Manager, and it directly determines how many total windows will be available per Report Channel to divide up between all radios that will use the channel. For more information on this topic, see the section called "Determining the Fast GPS Report Size".

2. How many total Fast GPS-enabled radios will use the site?

3. What is the Fast GPS Report Interval for the Fast GPS-enabled radios? This determines how many different radios can share the same Fast GPS Report Channel.

The next figure shows how the total system throughput for Fast GPS (in other words, the total number of reports per minute) is determined by:

1. The number of Report Channels available (as shown in the left-most column), and

2. The Report Size configured with the Network Manager. Even though all supported Report Sizes (5-10) are shown in the table below, each site in the same Connect Plus network should be configured for the same report size. It must be configured for the largest Fast GPS periodic report that will be transmitted by any Fast GPS-enabled radio.

3. Spacing between reports: The controller inserts 120ms of spacing between each window announcement. Since the announcement is sent on the Control Channel timeslot, but the report is sent on the FGPS Report Channel uplink, the spacing helps prevent collisions that could occur if radios assigned to consecutive timeslots (on the same Fast GPS Report Channel) did not trunk and transmit in the same length of time. Such timing differences are unavoidable and must be accounted for.

Report Channel Timeslots Needed	Report Size					
	5	6	7	8	9	10
1	142	125	111	100	91	83
2	285	250	222	200	182	166
3	427	375	333	300	273	249
4	570	500	444	400	364	332
5	712	625	555	500	455	415
6	855	750	666	600	546	498
7	997	875	777	700	637	581
8	1140	1000	888	800	728	664
9	1282	1125	999	900	819	747
10	1425	1250	1110	1000	910	830
11	1567	1375	1221	1100	1001	913
12	1710	1500	1332	1200	1092	996
13	1852	1625	1443	1300	1183	1079
14	1995	1750	1554	1400	1274	1162
15	2137	1875	1665	1500	1365	1245
16	2280	2000	1776	1600	1456	1328
17	2422	2125	1887	1700	1547	1411
18	2565	2250	1998	1800	1638	1494
19	2707	2375	2109	1900	1729	1577
20	2850	2500	2220	2000	1820	1660
21	2992	2625	2331	2100	1911	1743
22	3135	2750	2442	2200	2002	1826
23	3277	2875	2553	2300	2093	1909
24	3420	3000	2664	2400	2184	1992
25	3562	3125	2775	2500	2275	2075
26	3705	3250	2886	2600	2366	2158
27	3847	3375	2997	2700	2457	2241
28	3990	3500	3108	2800	2548	2324

Table 2-4 Fast GPS - Number of Reports per Minute Based on Report Size

Table 2-4 shows how many total reports can be transmitted per minute per Report Channel; it does not show how many different SU's are reporting.

To understand the number of different SU's that can be handled per report channel, it is also important to understand how the windows are numbered and how the periodic report interval influences the number of SU's that can share those windows.

The table below shows the number of different SU's that can be assigned to utilize a single Fast GPS Report Channel, depending on Report Size configured into the Network Manager and the Periodic Report Update Interval of SU's assigned to the channel.

Report Size	30 sec interval	1 min interval	2 min interval	4 min interval	8 min interval
5	70	140	280	560	1120
6	62	124	248	496	992
7	54	108	216	432	864
8	50	100	200	400	800
9	44	88	176	352	704
10	40	80	160	320	640

Table 2-5 Total SU's per Report Channel, by Report Size and Periodic Report Interval

In Table 2-5, the numbers shown in each column assume that all SU's assigned to the Report Chanel have the same periodic report interval. However, the controller can combine reports of different intervals (30 seconds through 8 minutes) on the same Report Channel. The System Administrator only needs to be concerned with enabling enough Fast GPS Report Channels to meet the total demand.

Report Size	Total Windows Shared by All SU's Assigned to Report Channel
5	1120
6	992
7	864
8	800
9	704
10	640

Table 2-6 Total Assignable Windows per Superframe at Different Report Sizes

Planning for the correct number of Fast GPS Report Channels per site is fairly straight-forward for a single-site network, once the system owner knows all of the following:

1. The largest Report Size that will be utilized by any Fast GPS radio. This determines the total number of available windows for each Fast GPS Report Channel.

2. The total number of radios that will be utilizing Fast GPS on the site.

3. The periodic report update interval for each Fast GPS SU.

However, planning the correct number of Fast GPS Report Channels per site for a multi-site network is more challenging because the number of radios that use each site at any given moment is not static. It changes as the Fast GPS radios roam from site to site in the Wide Area Network.

Therefore, when planning for the number of Fast GPS Report Channels per site in a multi-site network, it is recommended to plan for the "worst case" number of SU's that can possibly roam to the site at any one time. This helps assure that Fast GPS-enabled SU's can always be accommodated at the site.

In a simple example, let's assume a 2-site network that has 1400 Fast GPS-enabled radios, and every radio utilizes a Report Size of 5 and has a one minute report interval.

To account for the worst case scenario when one of the sites goes down and all radios roam to the remaining site, each site controller should be enabled (authorized) for ten Fast GPS Report Channels. The controller will not activate all ten Fast GPS channels unless they are needed. Until then, the channel can be used for voice and other data calls.

Assigning SU's to Fast GPS Report Channels

The System Administrator must plan for the correct number of Fast GPS Report Channels per site, but he/she does not need to assign specific radios to a specific Fast GPS Report Channels.

In Connect Plus Fast GPS, the radio's codeplug does not need to be programmed with the radio's Fast GPS Channel. Instead, the controller assigns the radio's Fast GPS Channel, window number, and frame number(s) dynamically, over-the-air, according to available resources at the time of assignment.

Assigning Fast GPS Report Channels and Windows

When a radio is enabled for Fast GPS in its user record, and when the Location application has sent the controller a Triggered Location Request with a supported periodic interval, the controller assigns a regular traffic channel (not a Fast GPS Report Channel) to deliver the Location Request to the radio and to receive the radio's first report. This is called the "Store Documents for Fast GPS Session". In this same session, the controller also provides the Option Board's Fast GPS Channel and window assignment. If the session does not complete successfully, the assignment is discarded and the session will be repeated. If the session completes successfully, the Fast GPS Channel and window assignment is considered valid, and the radio transmits its subsequent location reports on its assigned Fast GPS Report Channel at the interval requested by the application.

The Controller not only provides the radio with its Fast GPS Channel and window assignment in its "Store Documents for Fast GPS Channel" session, it also sends the assignment with every subsequent Registration Response. This allows the controller to provide the radio with an updated assignment, if needed. The Fast GPS assignment information does not increase the time required for a registration session.

The radio does not carry the same Fast GPS Report Channel and window assignment from site to site. A new assignment is provided when the radio registers with the new site, and is subject to the available site resources at time of registration.

Regardless of whether a radio receives its Fast GPS assignment in the "Store Documents for Fast GPS" session or in a subsequent registration session, the assignment info includes the following:

- The repeater and timeslot that this radio shall use to send Fast GPS periodic location reports.
- The window number that the radio shall look for when the controller sends Fast GPS announcements.
- The frame number(s) that the radio shall look for when the controller sends Fast GPS announcements.
- Additional information that the radio uses to determine whether its current assignment is still valid.

De-allocating Fast GPS Report Channels and windows

The controller de-allocates (removes) the Fast GPS Report Channel and window assignment(s) for a specific radio when:

- The same radio registers at a different site.

- The radio sends a power-down de-registration request, and the message is decoded by the controller.
- The location application sends a Triggered Location Stop Request for the radio, and when the controller informs the radio of the de-assignment.
- The location application’s Triggered Location Request times out (and is not refreshed by the application), and when the controller informs the radio of the de-assignment.
- The site controller reboots (which causes the controller to delete all assignments).

The controller de-allocates (removes) a Fast GPS Report Channel when:

- The controller has de-allocated the last Window assignment for the Report Channel, and there are no longer any radios assigned to the channel.
- The channel is no longer needed due to Report Channel Reallocation. See the discussion in a subsequent sub-section.
- The repeater is not responding to keep-alive messages, or has experienced a major alarm, or has been disabled via RDAC, or has been disabled by CPS for Remote Repeater Programming. See the discussion in a subsequent sub-section.

<u>How the controller selects which repeater timeslots to use as Fast GPS Report Channels</u>

The controller allocates Fast GPS Report Channels from the site’s pool of traffic channel resources based on several considerations:

- The controller allocates Fast GPS Report Channels on an “as needed” basis – up to the maximum number of allowed Fast GPS channels as configured in the Network Manager. If there are no registered SU’s that require Fast GPS updates, the controller will not allocate any channel as a Fast GPS Report Channel.
- When the first SU registers that requires a Fast GPS Report Channel, the controller converts one of the site’s regular traffic channels to a dedicated Fast GPS Report Channel. Once this occurs, the Fast GPS Report Channel can only be used for Fast GPS periodic Location Reports. It cannot be used for any type of voice or non-Fast GPS data.
- When the Controller assigns SU’s to a Fast GPS Report Channel, it is able to assign SU’s with different report intervals to the same Report Channel, provided that the necessary windows and frames are available. However, there are occasions when windows are available from some report intervals, but not for others.
- As additional SU’s register that require a Fast GPS Channel, the controller will load its existing Fast GPS channel as fully as possible. If the controller cannot locate available frame(s) and window(s) on an existing Fast GPS Report Channel, the controller will convert another regular traffic channel to a Fast GPS Report Channel. This process continues until the controller accommodates all Fast GPS SU’s, or until the controller cannot allocate any more Fast GPS channels (because the maximum allowed Fast GPS channels has been reached, or due to other logic checks in the controller).

Fast GPS Report Channel Overflow

If a SU is enabled for Fast GPS in its user record, but the controller cannot assign the radio to any Fast GPS Channel, the controller's operation at this point depends on whether the site has been enabled for "Fast GPS Overflow to non-Fast GPS Channel" (a configurable setting via Network Manager).

- If Fast GPS overflow is allowed (enabled), the controller makes a best-effort to obtain periodic location reports via non-Fast GPS method, utilizing unconfirmed location reports on a regular voice/data timeslot, subject to channel availability. This requires a Control Channel assignment message per report session. The controller also creates a SUID-specific Event Log entry upon scheduling the overflow session.

- If Fast GPS overflow is not allowed (disabled), the controller will not attempt to obtain periodic location updates from the SU, but it will continue to check for Fast GPS Report Channel and window availability each time the SU registers or re-registers with the site.

Configurable settings that help determine Fast GPS Report Channel utilization

The Network Manager provides configurable settings to help determine how many channels (and which specific channels) the controller will utilize as Fast GPS Report Channels:

1. The Network Manager provides a setting to determine how many Fast GPS Report Channels are allowed on a site. This number must be equal to or less than the number Fast GPS Report Channels that have been enabled (authorized) for the site.

2. The Network Manager provides the ability to configure a list of channels that should not be used as Fast GPS Report Channels (by repeater and slot). In configuring this "exclusion" list, the System Administrator should keep the following considerations in mind:

    a. Once the controller has allocated a Fast GPS Report Channel, the repeater downlink transmits continuously. This is necessary so that the reporting radios can quickly synch with the Fast GPS Report Channel, transmit their report, and then return to the Control Channel timeslot.

    b. It is advisable to avoid channels that are susceptible to frequent interference, which can disrupt the repeater's ability to receive data. When the repeater reports interference to the controller, the controller suspends reporting on the Fast GPS Report Channel until the repeater reports that the interference has cleared. Therefore, interference will reduce the number successful reports for the impacted Fast GPS Channel(s).

    c. The controller will not use timeslot 1 of any repeater that is on the Network Manager's Control Channel list as a Fast GPS Report Channel. Therefore, for any repeater on the Control Channel list, the Network Manager automatically checks (and grays out) the corresponding entry for timeslot 1 on the FGPS Report Channel Exclusion list.

Calculating and Configuring the Fast GPS Report Size

The Fast GPS Report size (5-10) is configurable in the Network Manager. The Fast GPS Report Size is the number of bursts required to transmit the datagram that includes the Fast GPS Periodic report and any additional overhead such as headers. The bursts are sent every 60ms, and each burst contains 30ms of data.

The Network Manager must be configured for the largest report size that will be transmitted by any Fast GPS-enabled radio that can possibly use the site.

It is permissible for radios to transmit a smaller report than configured in the Network Manager, but it is not permissible for a radio to transmit a larger report size than configured with the Network Manager.

Although the Network Manager provides a setting to configure the expected Report Size, neither the Network Manager nor the controller determines the radio's Fast GPS Report Size. This is determined by the location elements contained in the LRRP Request that is sent by the Third Party Location application.

In order to calculate the radio's Fast GPS report size, the Network Manager user must know which LRRP report elements are included in the location request (latitude, longitude, speed, etc.). Requesting more elements causes the radio to send a larger report, and therefore results in fewer periodic reports per report channel. Requesting fewer elements causes the radio to send a smaller report, and therefore results in more periodic reports per report channel. So, there is a tradeoff between how detailed a report is, and how many radios can be accommodated on the Fast GPS Report Channel(s). To maximize Report Channel throughput, it is recommended to request the minimum necessary set of GPS data.

It is also important to know the largest Request ID value that can be sent by the location application. For example, if the application utilizes values up to 65,535 for Request IDs, this can be expressed in two bytes. Once the maximum Request ID number is known, add an additional two bytes to determine the total impact of the Request ID element in the location report. For example, if the application allocates 2 bytes for Request ID numbers, then add 4 total bytes for Request ID. To determine the application's maximum size for Request ID numbers, please consult the application vendor.

The table below can be used to calculate the LRRP Response size. Once this is calculated, the total Response Size needs to be plugged into the equation to determine the Report Size in bursts. The calculation accounts for additional overhead such as headers and CRC error check.

When the Network Manager user knows the largest Report Size (in bursts) that will be sent by any Fast GPS-enabled radio, then he/she should enter this figure into the "Report Size" field in the Network Manager.

The Report size depends on the following factors:

- The parameters that the application has requested in a location response, such as longitude, latitude, time, altitude, velocity, direction, and so forth.
- The Request ID that the location application supplies in its location request.

Requested Element	LRRP Response Size (bytes)
Latitude + Longitude	11
Time	6
Request ID[14]	Maximum size of Request ID number (in bytes) sent by location application **+** 2
Speed_hor[15]	3
Direction_hor	2
Altitude[16]	3
Radius[17]	2
Beacon-maj-min-time	3 + 6 per reported beacon
Beacon-maj-min-txpwr-rssi-time	3 + 8 per reported beacon

To calculate the Report Size in bursts for Connect Plus Fast GPS Periodic Reports

1. Add the total number of bytes that have been calculated for LRRP Response size using the table above.

[14] Check with location application provider to determine the largest number that can be used for Request ID. This is a variable size field.
[15] Variable size field
[16] Variable size field
[17] Variable size field

2. Plug the total bytes for LRRP Response size into "LRRPResponseSize" into the formula supplied in the box below.

3. The result of the formula is the Report Size in bursts. If the result of the equation is not a whole number, then round up to the next whole number. For example, if the result of the equation is 5.2, then configure Report Size of 6 into the Network Manager.

Report Size in bursts = ((LRRPResponseSize + 1) ÷ 12) + 3

The formula above assumes that (1) unconfirmed datagram transmission is utilized, (2) that Privacy is not enabled, and (3) "Compressed UDP Data Header" is utilized. These are all true assumptions for Connect Plus Fast GPS.

It is vital that no Fast GPS radio transmits a report that is larger than the Report Size configured with the Network Manager. If this should occur, the report runs the risk of colliding with the report that is supposed to precede and/or follow the over-sized report. If such a collision were to occur, the controller may not decode either report, and may not know why it did not receive the report.

If the controller detects that the radio transmitted a report containing more bursts than the Report Size configured with the Network Manager, then the controller creates an SUID-specific Event Log entry to indicate the over-sized report. This should be investigated and corrected as soon as possible. The two possible ways to correct this are:

1. Re-configure the location application so that fewer location elements are requested for the SU that is sending the over-sized report. This can reduce the SU's report size so that it will fall within the Report Size configured into the Network Manager.

2. Increase the Report Size in the Network Manager. This will impact Report Channel throughput since it reduces the number of possible reports per Report Channel, per superframe.

Important! If the location report will include beacon information (used for indoor location tracking), then exercise care regarding the number of beacons requested. Requesting too many beacons can overrun the largest supported Fast GPS report size of 10 bursts. Also, do not request Beacon UUID since this data is too large for a Fast GPS Report.

Daily Report Channel Reallocation

Although the controller issues the Fast GPS channel and window assignments as efficiently as possible, over time the window assignments can become fragmented as the controller de-allocates assignments (due to radio powering down, registering with a different site, receiving a Stop Request from the location application, etc.) For this reason, Connect Plus supports daily Report Channel Reallocation. The Reallocation process allows the system to utilize its report channels more efficiently. Sometimes the controller is able to close down one or more report channels as a result of the reallocation process. If so, the channel is removed from the Fast GPS Report Channels, and is returned to the pool of traffic channels that are available to be used as normal voice/data resources. If Daily Reallocation is enabled and scheduled, then all radios will receive an updated Fast GPS assignment, even if the process does not reduce the overall number of Report Channels in use.

During Report Channel Reallocation, the controller sends a special superframe. **During this eight minute period, the Connect Plus radio does not transmit location reports**. Instead, the radio uses its Fast GPS window(s) to obtain an updated Fast GPS Report Channel and window assignment. If a radio does not obtain its updated Fast GPS assignment during the special eight minute superframe, it must re-register on the Control Channel for an updated assignment before it can resume its Fast GPS reports.

The Network Manager user enables Report Channel Reallocation, and schedules the time when Reallocation is performed. When enabled, Report Channel Reallocation is a daily event, and occurs as close to the scheduled time as possible (the controller must complete the current superframe before it starts the Reallocation process). It is recommended to schedule daily Reallocation during a time of day that has relatively low call activity, and when the eight minute pause in reporting will be the least impactful.

Fast GPS and Control Channel Rollover

Control Channel Rollover causes a brief interruption to Fast GPS window and frame announcements on the Control Channel downlink as the controller rolls from the previous Control Channel to the new Control Channel. It is important to know the following about Control Channel Rollover and Fast GPS:

1. The controller pauses the Fast GPS window announcements while switching control channels. This may extend the radio's report interval slightly (for the first report following rollover).

2. The controller remembers the last window and frame it announced on the previous Control Channel timeslot, and it starts Fast GPS announcements on the new Control Channel with the next window and frame.

3. Because radios enter Search during Control Channel Rollover, and must re-acquire the new Control Channel, the radio may miss a Fast GPS report due to Control Channel Rollover, especially if the radio's window and frame is one of the first to be announced on the new Control Channel timeslot.

4. Any radio that acquires the new Control Channel without sending a new registration request keeps its current Fast GPS Report Channel and window assignment. If the radio sends a new registration to the site after Control Channel Rollover (due to extended fade, or because it attempted to register with a different site), the controller sends a Fast GPS Report Channel window and frame assignment in the Registration Response. It may or may not be the same Report Channel and window assignment that the radio had previously.

5. For any site that has a scheduled time for Control Channel Rollover and a scheduled time for Fast GPS Report Channel Reallocation, **it is recommended to schedule the Fast GPS Report Channel Reallocation at least 30 minutes prior to the Control Channel Rollover**. This should provide sufficient time for the Fast GPS Report Channel Reallocation to complete prior to beginning the Control Channel Rollover.

Failure of Report Channel Repeaters

How the system handles Report Channel repeater failure depends on whether the Controller has regular traffic channels (on a good repeater) that it can convert to Fast GPS Report Channels. If so, then the controller can reassign the entire population of the failed report channel(s) to the new report channel(s). This feature is referred to as Report Channel Rollover, and it can be accomplished very quickly via a broadcast message sent on the Control Channel slot. It is not necessary to individually contact each radio.

Report Channel Rollover can be triggered by the following conditions. The list may not be all-inclusive:

- Repeater reports a significant alarm (one of the same alarms that would cause Control Channel Rollover)
- Repeater stops responding to keep alive messages, and the link times out.
- Repeater is disabled via RDAC command or by MOTOTRBO CPS (due to Remote Repeater programming)

If the controller does not have a regular traffic channel that it can convert to replace the failed report channel, then the controller makes a best effort to re-assign the SU's to available windows on other Fast GPS Report Channels. This process takes longer than Report Channel Rollover because the controller must individually communicate with each radio. In some scenarios, the Controller will not be able to re-assign the SU to a Fast GPS Report Channel due to lack of availability. If this occurs, and if Fast GPS Overflow is enabled, the controller creates a SUID-specific Event Log entry upon scheduling the overflow session, as previously discussed. Whether or not the

controller attempts to obtain the location reports via a non-Fast GPS traffic channel depends on whether Fast GPS Report Channel Overflow is enabled for the site (as discussed previously).

Missed Reports and Missed Reports Handling

Connect Plus does not (and cannot) guarantee that a radio will send a location report every time its assigned window and frame(s) is announced. This is for various reasons, including the following. This is not an all-inclusive list:

- If the radio is in a call when its assigned window and frame is announced on the Control Channel, the call-in-progress takes precedence and the radio will not report for that window/frame.
- If the radio user initiates a call just before the radio transmits the location report, the user-initiated call shall take precedence, and the radio will not report for that window/frame.
- If the radio is receiving over-the-air file transfer when its assigned window and frame is announced on the Control Channel, the radio will not report for that window/frame.
- If the radio is in a fade condition (out of coverage), it may not decode its window/frame announcement on the Control Channel downlink. In this event, the radio will not report for that window/frame.
- If the radio hears its window/frame announcement on the Control Channel, but is out of transmit range for its Fast GPS Report Channel, the radio will make an effort to transmit its location report on its Fast GPS Report Channel, but the radio's transmission may not be decoded by the Report Channel repeater or by the controller. Such a condition is referred to as "unbalanced coverage" and is more common with portable radios than with mobiles. If this occurs with regularity, it is a symptom of faulty system design, and should be corrected as soon as possible.
- If the radio was powered-down, but the controller didn't decode the de-registration message, the controller will expect a report, even though the radio won't send one.
- If the battery on the radio or vehicle runs down, the radio cannot transmit reports, and it cannot notify the controller that it is unavailable. Therefore, the controller will expect a report, even though the radio can't send one.

In Connect Plus Fast GPS, once the radio attempts to transmit a location report, it does not store or retain the report. Also, if the radio cannot transmit a location report, it does not store or retain the radio's location information for the un-reported interval.

Occasional missed reports are part of normal operation and should not cause undue concern. In most cases the radio will report in a subsequent Fast GPS window (sending fresh GPS location information). However, if the radio misses multiple consecutive reports, this becomes more noticeable. For this reason, Connect Plus supports a feature called "Fast GPS Missed Reports Handling".

"Missed Reports Handling" is enabled via the MOTOTRBO Connect Plus Network Manager. When enabled, the controller tracks how many consecutive Fast GPS reports it has missed from each SU assigned to a Fast GPS channel. If the number of missed reports hits the "Missed Reports Threshold" value that has been configured with the Network Manager, the controller schedules a make-up report session on a normal traffic channel. The session will be assigned with a SUID-specific Control Channel message. The traffic channel session utilizes an unconfirmed datagram to minimize the time required for the report. The controller will not schedule the traffic channel session if it knows the SU is involved in a call.

If the SU sends a location report, either during its scheduled Fast GPS Report Channel window or during a Missed Report session, the controller sets the radio's missed Reports counter back to zero upon receiving the report.

If the SU does not send a Fast GPS report because the controller has suspended reporting on the radio's Fast GPS channel, then the controller does not increment the Missed Reports counter. The controller suspends reporting in the following scenarios:

- Reporting is suspended while the repeater is performing analog Base Station Identification (BSI).
- Reporting is suspended due to interference on the Fast GPS Report Channel.
- Reporting is suspended because the Report Channel has a significant repeater alarm (one of the same alarms that would cause Control Channel Rollover), or because RDAC has disabled the repeater, or because MOTOTRBO CPS is using the repeater for Remote Repeater programming, or because the repeater has stopped responding to "keep alive" messages and the link has timed out, etc.

When Missed Reports handling is enabled, the "Missed Reports Threshold" is configurable for each supported report interval (30 seconds through 8 minutes). Caution is recommended when enabling Missed Reports Handling and when configuring the Missed Reports Threshold value. If there are a large number of SU's that must be scheduled for Missed Report sessions, this could have a detrimental impact on other types of calls due to the competition for traffic channels and Control Channel messages.

Monitoring Fast GPS Performance

Since the goal of Connect Plus Fast GPS is to obtain location reports that can be displayed and tracked via a location application, one means of tracking Fast GPS performance is to watch whether the radio's location updates as expected on the application's tracking screen. However, since there are several reasons why a radio's position may not be updated (including a blocked view of the sky), it is sometimes helpful to look at controller data for more information.

The controller tracks several types of Fast GPS Data, and provides the same data in three alternative formats:

- **Fast GPS Tracking Window**, launched via the Network Manager:
  It is updated every 30 seconds, and shows Fast GPS data for the assigned windows in the superframe. Due to the volume of data that must be communicated between the controller and the Network Manager, the display only shows information for one Fast GPS Report Channel at a time. More information is provided on the Fast GPS Tracking window in subsequent paragraphs.
- **Fast GPS Historical Data**, saved to hard disk:
  When enabled via the Network Manager, the site controller saves up to 100 MB of Fast GPS Data for all Report Channels to the controller's hard disk. If the data exceeds 100 MB, the oldest data is automatically deleted and replaced with the newest data. To prevent data from being lost, the Network Manager user can download the data from the controller's hard disk to a computer before it is automatically deleted by the controller, or the data can be automatically exported to a XRT Gateway Client application (see next paragraph).
- **Fast GPS Historical Data**, automatically exported to XRT Gateway Client Application:
  When requested by an XRT Gateway device, the XRC Controller automatically exports the Fast GPS Data for all Report Channels to the requesting XRT Gateway. The XRT will forward the data to the XRT Client application that initiated the request. The controller sends Fast GPS data to the XRT Gateway approximately 30 seconds after a frame ends, and each update contains 30-seconds worth of new data about a specific frame.

Fast GPS Tracking window

The following bullets discuss the Fast GPS Data in context of how it is displayed by the Network Manager's Fast GPS Tracking window. The same data set is supplied in the alternative formats, but may not be displayed in the same fashion.

- The Fast GPS Tracking window displays a grid that represents the Fast GPS superframe. The columns in the grid represent the frames (1-16) and the rows in the grid represent the windows. The number of windows per frame varies according the Report Size configured in the Network Manager. The intersection of the columns (frames) and the rows (windows) represent the individual cells within the superframe.

- The Network Manager Fast GPS Tracking Display shows one superframe of Fast GPS data for the requested Report Channel. The Network Manager updates the displayed information one column of data (i.e. one frame of data) at a time. Statistical data is reported by the controller approximately 30 seconds after a frame ends, and each update contains 30-seconds worth of new data about a specific frame. The Network Manager provides an information bar above the grid display that contains a date and time stamp for when the grid was last updated, and it contains the frame number for the last updated frame. If the last updated frame was 5, for example, then the columns for frames 1-5 contain information that has been updated during the current superframe. The columns for frames 6-16 contain information that was last updated during the previous superframe. Whenever the Network Manager receives updated information for a frame, it overwrites any information that was previously displayed for the same frame number.

- For each cell in the superframe, the Network Manager displays the SUID of the radio currently assigned to the cell. If there is no radio currently assigned to a cell, the Network Manager displays “Unassigned”.

- For each assigned cell, the Network Manager displays the percentage of reports received for the cell as compared to the number of announcements the controller has sent for that specific SUID/window/frame combination. The calculated percentage is the percentage for this specific cell since it was assigned to this specific SU. The percentage is reset after each controller reboot, when the corresponding Fast GPS Report Channel is reallocated, or when a different SUID is assigned to the window. When interpreting the displayed percentage, it is important to understand the following:

    - Unless the radio has an eight-minute report interval (which means that it only has one assigned cell per superframe), it is not possible to determine the radio’s overall “reports received percentage” by reading the percentage of a single cell. To calculate the radio’s overall “reports received percentage”, it will be necessary to consider all of the cells assigned the same radio within the superframe. This will be as many as 16 cells within the superframe for a radio with a 30-second report update interval.

    - When the system calculates the “received reports percentage”, a “received” report is any LRRP response received from the radio, even if the response doesn’t contain valid and/or current location data (due to lack of a satellite fix or other reasons).

- When the Fast GPS Report Channel Tracking window contains additional information about a specific cell, the cell is highlighted and an exclamation point icon appears within the cell. Holding the mouse pointer over the exclamation point icon causes the Network Manager to display a message pertaining to this specific cell. Some of these messages explain why the controller didn’t receive a report for this cell. It should be noted that:

    - Occasional missed reports are a normal part of Fast GPS operation. For more information, see the sub-section called “Missed Reports and Missed Reports Handling.”

    - Sometimes the controller doesn’t know why it didn’t receive a report in a specific cell. In this case, the exclamation point icon is not displayed, and the Network Manager doesn’t display any message containing additional information.

- The following are examples of scenarios of when the controller knows why a report was not received for a specific window/frame, and Network Manager provides a message in the Tracking window.

    - The repeater was performing Base Station Identification during this window/frame.

- The repeater was experiencing interference during this window/frame.
- The controller knows that a call was taking place on one of the radio's registered IDs during this window/frame. Sometimes the controller doesn't know when the radio is already listening to a different call (such as when the radio has scanned into a call on a Group to which it isn't registered, or when the radio has joined a Network Frequency File or Option Board firmware over-the-air file transfer). For such cases, the system does not provide any special message to the Network Manager user.

- If the controller detects a report in this cell that is larger than the Report Size configured with the Network Manager, the application will display a message to this effect when the Network Manager user holds the mouse over the exclamation point. For more information about this issue, and how to resolve it, see the sub-section called, "Calculating and Configuring the Fast GPS Report Size."

The Network Manager Real Time Display shows which repeaters and slots are currently serving as Fast GPS Report Channels, but it does not show which radios are assigned to the channel, or when reports are received (or not received) from radios assigned to the channel. This controller tracks this information in the Fast GPS Historical Data.

The downloadable airtime call log does not provide any information on Fast GPS Report Channels, or Fast GPS Report Sessions. This controller tracks this information in the Fast GPS Historical Data.

2.7.13 Connect Plus Indoor Location Tracking

Beginning with System Release 1.7 (R2.6.0), Connect Plus supports the ability to report iBeacons detected by the radio's Bluetooth receiver. This technology can be used to track a radio's location in places where the GNSS/GPS satellite signal cannot normally penetrate.

The following bullets briefly summarize how the feature works:

- The customer obtains iBeacon devices. The iBeacon is a low-power device that transmits an "advertisement" message, which repeats at a configurable interval and utilizes BLE (Bluetooth Low Energy) technology. The "advertisement message" contains a user ID code consisting of three parts; UUID, Major and Minor. Many devices can (and often) share the same UUID. Multiple devices within the same UUID can also have the same Major version. However, every device should be configured with a unique UUID/Major/Minor ID combination so that the decoded "advertisement" message can be associated with a specific iBeacon device. As a simple example, the UUID might represent an area encompassing multiple buildings, the Major might represent a building (or section of a building), while the Minor identifies a specific beacon device, at a specific location, within a specific room. To track a radio's indoor location, the location application must know the UUID/Major/Minor ID and the exact location of each individual beacon device. The "advertisement" message also includes the device's transmit power. The application can use this information, in conjunction with the receive signal strength (RSSI), to determine the radio's approximate distance from the beacon transmitter.

- The customer obtains and loads "Indoor Location Tracking" feature licenses for all radios that will be using the Indoor Location feature.

Each radio that will be utilizing the Indoor Location feature has several MOTOTRBO CPS configurable settings associated with the feature:

- The ability to enable/disable Indoor Location scan.

- Configurable timers for Scan Interval On and Scan Interval Off. When configuring these timers, consider the interval that advertisement messages are transmitted by the iBeacon devices. The more time that the radio spends scanning for beacons, the greater the impact on battery usage.
  - The ability to configure between 1 and 20 UUIDs that the radio should respond to when scanning and storing Beacon data. Messages that have a non-matching UUID are discarded by the radio. Enter the desired UUID(s) with care, using hexadecimal characters.
  - The ability to enable the “Indoor Location” menu option. When enabled, Indoor Location can be enabled/disabled from the radio’s Bluetooth menu. This also enables the Beacon Detail menu option. Beacon Details shows the UUID, Major, Minor, and RSSI information for the five most recently decoded beacons.
- MOTOTRBO Connect Plus CPS (CP CPS) supports a programmable button to enable/disable Indoor Location.
- Disabling Indoor Location can help conserve battery (by disabling the Beacon scan function), but it will not stop the Connect Plus controller and Option Board from attempting to obtain Location Reports containing Indoor Location data, if so requested by the location application. Indoor Location Data that is sent to the location application when Indoor Location is disabled will not be current.
- When Indoor Location is enabled in a BLE-capable subscriber radio, it scans for iBeacon messages that contain an expected UUID. Upon detecting such a message, the radio makes an entry in an internal list of detected Beacons. Each list entry contains the beacon’s ID (UUID, Major, Minor), the beacon transmit power, the signal strength (RSSI) of the decoded beacon, and a timestamp affixed by the radio. The timestamp indicates how many seconds had elapsed since radio power-up when the radio decoded the Beacon. It is useful for ordering beacon reports from the same SU, but cannot be associated with clock/calendar time until additional time information is affixed by the location application upon receiving the report.
- The radio’s internal list of scanned beacons can contain entries for up to 200 decoded beacon messages. The beacons are stored in “First In First Out” order.
- The Location application can request the radio to report a specific number of detected beacons from its list. The Location application can also specify which data should be sent with each Beacon entry. Major, Minor, and Timestamp are normally requested. RSSI, Transmit Power and Beacon UUID can be added to this data set, if desired. It is usually unnecessary to request Beacon UUID, and this should never be requested for a Fast GPS Location Report due to the size of the resulting report.
- Upon receiving a LRRP report, the application can affix its own timestamp to associate the report with clock time and processes the Beacon data. Assuming that the application already knows the location of each iBeacon device, the application can derive the SU’s approximate location and movement by processing the data in the LRRP report.

There are several important things to understand about how GNSS/GPS (Outdoor) Location and Beacon (Indoor) Location work together and interact:

- The LRRP protocol provides the flexibility to request both GNSS/GPS and Beacon Location elements in the same location report, if desired. The following sub-bullets assume that the target radio has hardware, software, and feature permission to support both GPS and Beacon location data:
  - A single (immediate) location request can contain Beacon elements only, GNSS/GPS elements only, or a combination of both.

- The Connect Plus radio supports one Triggered Request with Emergency Trigger at a time. The request can contain Beacon elements only, GNSS/GPS elements only, or a combination of both.

- The Connect Plus radio supports one Triggered Request with Periodic Trigger at a time. The request can contain Beacon elements only, GNSS/GPS elements only, or a combination of both.

- When utilizing Fast GPS, the application (and/or application user) should exercise care regarding the number of beacons requested. Requesting too many beacons can overrun the largest supported Fast GPS report size of 10 bursts. It is the responsibility of the application (and/or application user), to know the resulting report size prior to deciding which elements (and how many elements) to include in the location request. See section "*Connect Plus Fast GPS*" for a table and formula that can be used to calculate LRRP report sizes.

2.8 Connect Plus Over-The-Air File Transfer

For certain types of Connect Plus files, the Connect Plus system provides two options for transferring the file to an SU:

- Connect Plus CPS can be used to transfer the file from a PC to the SU, utilizing the standard MOTOTRBO radio programming cable. This approach, sometimes referred to as "tethered programming", is the recommended method for initial set-up and programming. It can also be utilized following deployment to the field.

- The file can be uploaded to the Connect Plus controller, and then transferred over-the-air (OTA) to Connect Plus SU's. This feature, available only in Connect Plus, can reduce radio down time when the SU needs to be updated with a new file version after it has already been deployed to the field.

The following sections explain how OTA File Transfer works in this Connect Plus release. In the future, additional file transfer options may be offered.

2.8.1 Supported File Types

The following file types are supported for Connect Plus OTA File Transfer:

- Connect Plus Network Frequency File

- Connect Plus Option Board firmware

- Connect Plus Option Board Codeplug

Note: Connect Plus Option Board firmware files use either the *.efo or *.efb file extension, depending on the radio model. To determine which Option Board firmware file extension is required by a specific model, use one of the following methods:

- For any type of supported model: Open the MOTOTRBO Connect Plus CPS Help File and refer to the list of supported Radio Model Numbers in Appendix A. This list shows the Option Board firmware file extension required for each supported Model Number.

- For display models: Discover the required Option Board firmware file extension via the menu, by using one of the following sequences (depending on radio model):

- Menu→ Utilities→Radio Info→Opt. Bd FW Ver.
  OR
- Menu→Utilities→Radio Info→Versions (and then look for OB FW Version on the list)

- After following the appropriate menu sequence above, the display will show the Option Board firmware file version number followed by a file extension in brackets; [.efo] or [.efb].

If a site or network has a mixture of radio models that utilize different Option Board firmware file extensions, and if all models need to be updated with new Option Board firmware over-the-air, it will be necessary to perform a separate OTA firmware file session (one-at-a-time) for each Option Board firmware file with a different file extension. A Connect Plus radio only joins the over-the-air session if all of the following are true: (a) the radio has been configured with Connect Plus CPS to allow OTA firmware upgrades, (b) the session matches its expected Option Board firmware file extension and (c) the version that is being sent is newer than the Option Board's current firmware file version (unless OK to downgrade is checked).

2.8.2 OTA File Transfer Settings for MOTOTRBO CPS

Even though OTA File Transfer is only available in Connect Plus mode, there are some MOTOTRBO CPS settings that are important to its operation. This is because Connect Plus uses MOTOTRBO data transfer as the transport mechanism for file packets. The following MOTOTRBO CPS settings affect Connect Plus OTA File Transfer:

- The Connect Plus **Radio ID** is set with MOTOTRBO CPS. Select a Radio ID between 1 and 16776351 that has not been used for any other radio in the Connect Plus network. The Radio ID is used as the Destination ID for OTA File packets sent to this Connect Plus SU.

- Connect Plus requires that the **CAI Network** and **CAI Group Network** settings must be left at the default values.

- Set **Max TX PDU** to accommodate the largest text message, data message, or LRRP Report transmitted by the radio while operating in a Connect Plus zone. The recommended value is 500 bytes or larger. If the radio is capable of sending a 280 character text message, set Max TX PDU to at least 750 bytes. Set to 1500 bytes to accommodate maximum possible location report size containing indoor location elements.

- **TX Preamble Duration** determines the length of the preamble that is sent before IP datagrams transmitted by the SU. This value should be set to **zero**.

- For Connect Plus digital channels, **Compressed UDP Data Header** should be disabled (unchecked)

- For Connect Plus Channels, **Data Call Confirmed** should be enabled (checked)

2.8.3 OTA File Transfer Settings for Connect Plus CPS

There are several programmable parameters in the Connect Plus codeplug for OTA file transfer. The following parameters are configurable per Connect Plus SU (using Connect Plus CPS). They must be configured prior to field deployment.

- **Enable OTA File Transfer**: This setting defaults to off, meaning that OTA File Transfer is disabled for Option Board Firmware File and Network Frequency File. Because these OTA file types are targeted at the general radio population, and not at specific SU's, they can unexpectedly prevent a radio user from

receiving calls for a period of time. For this reason, it may be advisable to leave this setting disabled for some Mission Critical users. When disabled, file transfer for Option Board Firmware and Network Frequency File can only occur via the traditional method using Connect Plus CPS and a programming cable. When enabled, the Connect Plus SU can acquire these file types via OTA File Transfer. This setting does not affect OTA Transfer of the Option Board codeplug. The System Administrator grants permission for Option Board codeplug OTA transfer to take place by acknowledging a Network Manager message when uploading a new Option Board codeplug for a specific radio. Although the Codeplug File OTA transfer can also prevent the SU from receiving calls, it is the System Administrator’s responsibility to communicate with the radio user, and to perform the Codeplug File Transfer when a temporary interruption to service can be tolerated.

- **OTA Update Upon Completion**: When the radio completes OTA Option Board Firmware file transfer, this setting determines when the radio will update (upgrade) to the newly acquired firmware file. When enabled, the Option Board shall upgrade immediately upon completing the OTA File Transfer. If not enabled, the upgrade will be automatically performed the next time the radio is powered-up in an Option Board zone. While the radio is updating (upgrading) to the newly received firmware file, the user will not be able to make or receive calls. For the Network Frequency File and the Option Board Codeplug File, the Option Board always automatically and immediately upgrades to the new file after completing OTA File Transfer and verifying the integrity of the received file. Automatically upgrading to a new Network Frequency File received OTA does not typically interrupt service (provided that the frequencies currently being used by the SU haven’t changed). Automatically upgrading to a new Option Board Codeplug File received OTA does result in a temporary interruption of service as the Option Board loads the new codeplug and re-registers with the network. For this reason, it is the System Administrator’s responsibility to communicate with the radio user, and to perform the Codeplug File Transfer when a temporary interruption to service can be tolerated.

- **Unconfirmed File Transfer Dwell Time**: During Unconfirmed File Transfer this value determines how long the radio will remain on the trunk-to timeslot without decoding any valid file packets. If the timer expires and no valid packet is decoded, the radio returns to the Control Channel timeslot. If the OTA File Transfer was for Option Board Firmware or the Network Frequency File, the Option Board starts its “File Transfer Attempt Interval Time” upon returning to the Control Channel timeslot.

- **File Transfer Attempt Interval Time**: When the radio has been involved in an Option Board Firmware or Network Frequency File OTA Transfer, and it leaves the trunk-to timeslot with an incomplete file (for any reason), the radio starts the File Transfer Attempt Interval Time. The timer must expire before the radio will automatically attempt to resume the file transfer. A display radio user can request the radio (via the menu) to resume the file transfer prior to expiration of the timer.

2.8.4 OTA File Transfer Configuration in the XRC Controller

The first step to configuring OTA File Transfer in the XRC controller is to acquire the file that will be uploaded to the controller for OTA transfer. The file should be placed in a known location on the PC that will be used to upload to the controller. The PC must have the MOTOTRBO Connect Plus Network Manager software, and it must be configured to talk to the desired Connect Plus site(s).

Once the file is placed in a known location on the PC, the steps are as follows:

1. Launch the Connect Plus Network Manager Connection Tool and connect to the Connect Plus Site.

2. From the Main Menu, select Site Control/Upload, and then the desired File Type.

3. Press “File to Send”. This opens a window used to locate the file on the PC.

4. Browse to the directory containing the file for upload, select the file, and press “Open”.

5. For the Option Board Codeplug File, the user may then press, “Upload”. The Network Manager will perform several checks prior to uploading the file. The user will be informed whether or not the upload was successful.

6. For the Option Board Firmware File and the Network Frequency File, it is necessary to configure several additional parameters prior to pressing “Upload”:

- **Time to Beacon:** Determines how long the controller will “beacon” a special control channel message to inform SU’s of file availability. This time must be equal to “Time to Dedicate”. This message should not be confused with the IP Site Connect Beacon, which is not used in Connect Plus.

- **Time to Start:** Tells the controller when to start sending the File Beacon message (date and time). The controller also starts the dedicated channel file transfer at the configured date and time. Enter a date and time by typing over the current information. As a convenience, click the arrow to view a drop-down calendar that can be used to select the desired date. The time can only be entered by typing over the current time. The date and time values configured into “Time to Start” are based on PC local time. When uploading the file to the XRC, the Network Manager converts the configured values to UTC time. The controller will then start the file transfer at the requested UTC date and time according to the controller’s internal clock. The PC used to upload the file must be in synch with the XRC in regards to UTC time. If they are not in synch, the file transfer may start at a different time than is expected by the Network Manager user. If the configured time is in the past according to the controller’s clock, the file transfer will not take place at all. In order for the PC and the XRC to be in synch, both of the following must be true: (a) The PC date and time must be correct for the Time Zone that is configured on the Microsoft Window’s Date and Time Properties screen, and (b) the XRC clock must have the correct date and time in UTC. The controller’s date and time in UTC can be viewed with the Network Manager (*Settings→Date & Time*).

- **OK to Downgrade:** When checked, the controller sets a bit in the File Beacon message telling the Connect Plus SU that it is OK to downgrade to this file from a higher version. By default, “OK to Downgrade” is not enabled, and this is usually the recommended setting. Even if the box is checked, the Option Board is coded with certain rules that may not allow a downgrade in some circumstances.

- **Dedicated Channel (checkbox)**: Check this box to enable a Dedicated Channel file transfer. This is the only type of OTA File Transfer currently supported for Option Board Firmware File and Network Frequency File. During Dedicated Channel transfer, the controller will dedicate a specific repeater and timeslot for unconfirmed file transfer for the period of time specified. The file will be sent on the dedicated timeslot over and over until the “Time to Dedicate” expires. When checked, the software activates the Dedicated Channel options (Repeater Radio ID, Repeater Slot, and Time to Dedicate). **Note**: For Option Board Codeplug File OTA Transfer, it is not necessary (or possible) for the user to select the repeater and slot. The XRC automatically selects the repeater and slot.

- **Repeater Radio ID:** Enter the Radio ID (1-15) of the repeater that will be used for the dedicated channel transfer.

- **Repeater Slot:** Enter the Repeater Timeslot (1 or 2) of the trunk-to timeslot that will be used for the dedicated channel transfer. The Control Channel timeslot (and currently active Fast GPS Report Channel timeslots) should not be used.

- **Time to Dedicate:** Determines how long the repeater and timeslot configured above will be used for the dedicated channel file transfer. From “Time to Start” until “Time to Dedicate” expires, the dedicated slot will not be available for regular calls. SU’s may join or leave the dedicated channel transfer at various times (the radio user can cancel out of the transfer). It is recommended that “Time to Dedicate” should be set at least long enough so that the controller can send (at a minimum) three complete iterations of the file. The longer this value is set, the greater the chance that the largest possible number of radios can

acquire the file via unconfirmed data transfer. A setting of 65,535 minutes tells the controller that the dedicated channel transfer should never expire. **Important**: “Time to Beacon” must be equal to “Time to Dedicate”.

7. Press “Upload” to begin uploading the file to the controller. **Note**: This process must be completed at each site where the file will be available for OTA File Transfer.

Note: The XRC processes one Beaconed File Transfer (Option Board Firmware File or Network Frequency File) at a time. Do not upload a second file of either type until the XRC has either transmitted or deleted (in the case where it cannot transmit or finish transmitting) any previously uploaded file.

2.8.5 Controller File Handling for OTA Transmission

After receiving the uploaded file, the controller breaks the file into multiple IP data packets for OTA transmission. The number of data packets depends on the file size. File packets do not have to be collected in order, and the Connect Plus radio will not attempt to use the new information until it has received all file packets and checked the integrity of the received data.

2.8.6 OTA File Transfer: Unconfirmed File Transfer

Unconfirmed File Transfer refers to a method of transferring data over-the-air where the receiving radio does not individually acknowledge each received packet. This method of data transfer provides the highest available Forward Error Correction (FEC) rate. In Connect Plus, unconfirmed file transfer can be broken two categories:

1. **Beaconed File Transfers**: Files in this category are the Option Board Firmware File and the Network Frequency File. This type of File Transfer is intended for all members of the general radio population that need the “Beaconed” file. Because it is intended for multiple radios, there is no OTA acknowledgement of received packets, and there is no OTA acknowledgement that the SU has received the entire file.

2. **Targeted File Transfers**: This type of OTA File Transfer is targeted to a specific Radio ID. At the current time, the Connect Plus Option Board Codeplug is the only supported file type for Targeted File Transfer. Although the radio does not acknowledge each received packet (which places it in the category of unconfirmed data), it does send an OTA message to confirm receipt of the entire file.

2.8.6.1 Beaconed File Transfers

Beaconed File Transfer (Option Board Firmware File and Network Frequency File) allows many radios to receive file packets at the same time on the same trunk-to timeslot. It is initiated when the Network Administrator uploads a file for OTA Transfer that has been configured with the following attributes (see OTA File Transfer Configuration in the XRC Controller for more information on these settings):

- Time to Beacon has been set to indicate how long the Beacon message should be sent to announce file availability.
- A dedicated repeater and timeslot has been configured for the dedicated channel file transfer.
- Time to Start has been set to indicate when the controller should start sending the Beacon message on the Control Channel Timeslot and when the controller should start transmitting the file on the dedicated repeater and timeslot.

The following steps describe how the Beaconed File Transfer process works:

1. The SU is idle and monitoring the Control Chanel timeslot. It decodes a File Beacon message announcing file availability. It checks the File Type and version against what it currently has. If the version in the Beacon message is older than what the radio already has, it will NOT proceed to acquire the file unless the "OK to Downgrade" flag is set in the File Beacon message.

2. If the SU determines that it needs the file, it looks to see if the Beacon message gives a dedicated repeater and slot. If so, the SU will automatically move to the dedicated timeslot and start to acquire file packets.

3. On the trunk-to timeslot, the SU begins to acquire and store file packets. Because this is an unconfirmed transfer, possibly involving many radios, the controller does not request or expect OTA acknowledgement for transmitted packets. As long as a display-capable SU remains on the dedicated channel collecting packets, its display toggles between the Selected Contact Name and "File Transfer". The collection of packets continues until one of the following occurs:

    a. The radio user starts a call. This causes the SU to leave the file transfer.

    b. The SU collects all file packets.

    c. The Time to Dedicate Repeater expires and the File transmission ends.

    d. The SU's "Unconfirmed File Transfer Dwell Time" expires and the SU hasn't decoded a valid packet

4. When the SU leaves the dedicated timeslot, for any reason, it returns to the Control Channel timeslot.

    a. If the SU leaves the dedicated timeslot without collecting all needed packets, it starts its configurable "File Transfer Attempt Interval Timer". The SU will not automatically re-join an ongoing dedicated channel transfer until this timer expires. If the timer expires, and the Beacon message indicates that a dedicated channel transfer is still in progress, the SU will rejoin the transfer exactly as described above. Depending on factors such as signal conditions and how often the radio user wishes to initiate calls, this process may have to be repeated several times before the radio collects all necessary packets.

    b. If the SU leaves the dedicated timeslot after collecting all necessary packets, it will not update (upgrade) to the new file until it has checked to verify the integrity of the received data.

Note: If the Dedicated Channel Unconfirmed File Transfer expires before all radios have collected the complete file (display radios have a menu option to show whether the Connect Plus SU has collected all of the file packets), there are two options for completing the file transfer; (a) re-start the Dedicated Channel Unconfirmed File Transfer by re-configuring and re-uploading the desired file, or (b) update the radio(s) with the desired file via the traditional method using a programming cable and MOTOTRBO Connect Plus Option Board CPS.

2.8.6.2 Targeted File Transfer

Targeted File Transfer provides the ability to send files OTA to specific Destination ID(s). At the current time, Option Board Codeplug File Transfer is the only type of supported Targeted File Transfer.

Option Board Codeplug File Transfer

Option Board Codeplug File Transfer provides the ability to update the Option Board codeplug of a specific Connect Plus SU over-the-air. The discussion on OTA Option Codeplug File Transfer will be divided into four parts:

1. Creating the Option Board Codeplug File for OTA Transfer
2. Locating the destination SU and initiating Option Board Codeplug File Transfer
3. The Option Board Codeplug File OTA Transfer Process
4. Determining whether or not the Codeplug File Transfer was successful

Creating the Option Board Codeplug File for OTA Transfer

The process begins by using MOTOTRBO Connect Plus CPS to create and save the codeplug that will be sent OTA. The process is outlined below:

1. There are two saved formats for Option Board Codeplug Files, and each format has a different file extension, as shown below. In preparing a codeplug file for OTA Transfer, you can start with a saved codeplug in either format. After you open the codeplug and make any desired changes, you must save the file to the .efc file extension (by selecting *Save As→OTA Codeplug*).

   - **.cno** file extension: This type of codeplug file can be sent to the Option Board using a PC, the programming cable, and Connect Plus CPS. When saving to this format with Connect Plus CPS, the user defines the file name.

   - **.efc** file extension: This type of codeplug file can be sent to the Option Board over-the-air, after first uploading the file to the XRC using the MOTOTRBO Connect Plus Network Manager. When saving to this format with Connect Plus CPS, the software automatically names the file, using a specific format. It must not be changed by the user.

2. It is not necessary to start with a codeplug that matches the destination radio's SUID exactly. It is allowable to start with a sample codeplug, or with a saved codeplug from a different radio, <u>provided that the starting codeplug exactly matches the Model Number Index of the destination SU</u>. The best way to determine the Model Number Index of the destination SU is to instruct the radio user to look on the menu under *Utilities→Radio Info→Model Index*. If this is not possible, and if there is a recent saved Option Board codeplug available for the same SU, the Model Number Index is displayed on the Connect Plus Option Board screen when viewing the saved codeplug with Connect Plus CPS.

3. Every Option Board codeplug has a Codeplug Version Number. The codeplug that will be sent OTA must be the Option Board Codeplug Version required by the destination unit. The unit's Option Board Firmware level determines what Codeplug Version it needs. The best way to determine the necessary Option Board Codeplug Version is to instruct the radio user to look on the menu under *Utilities→Radio Info→Opt Bd CP Ver*. If this is not possible, and if there is a recent saved Option Board codeplug available for the same SU, then open the saved codeplug. The Option Board Codeplug Version is displayed on the Connect Plus Option Board screen when viewing the codeplug with Connect Plus CPS. However, it is important to realize that the saved codeplug might not contain the Option Board's

current information. For this reason the Menu display is preferable. After determining the Codeplug Version that the Option Board needs, confirm that the current Connect Plus CPS saves codeplugs to this Codeplug Version. If it doesn't, it may be necessary to locate an older or newer version of Connect Plus CPS.

4. Although it is not necessary to start from a saved codeplug that matches the Radio ID (SUID) of the destination unit, it will be necessary to enter the destination SUID when saving the codeplug for OTA transfer. Connect Plus CPS will automatically include the Destination SUID as part of the file name. The saved codeplug can only be utilized for the specific SU indicated in the file name. Therefore, if there are multiple SU's that need to be updated OTA with new codeplugs, it will be necessary to create a separate saved Option Board Codeplug File for each SU.

The guidelines shown above must be followed exactly for the OTA Codeplug Transfer to be successful. Because of this, the System Administrator is advised to maintain a spreadsheet or database for each deployed radio that contains, at a minimum, the following information for each unit; MOTOTRBO Serial Number, Radio ID, Radio Model information, the radio's Physical Serial Number, current Option Board Codeplug Version, current MOTOTRBO and Option Board software versions. This information will prove invaluable when creating Option Board Codeplugs for OTA Transfer.

When saving a file to the OTA Codeplug format (.efc file extension), Connect Plus CPS automatically names the file, using a specific format. It must not be changed by the user. An example of the file name as set by Connect Plus CPS is as follows: SU_204_7_A1B2C3D4.efc.

- **SU**: This indicates that the saved file is for a SU.
- **204**: This indicates that the saved file is for Radio ID 204
- **7**: This is an example of the Radio Model Index Number. It will likely be different for different radio models.
- **A1B2C3D4**: This is an example of the hexadecimal CRC of the saved codeplug. This information is useful for determining whether the destination Option Board successfully receives this Codeplug File OTA. Following the transfer, request the radio user to check the CRC of the Option Board OTA Codeplug File: *Utilities→Radio Info→OB OTA CPcrc*. This menu option is available on display radios when the Option Board's current codeplug was received OTA. Selecting this option causes the Option Board to display the OTA Codeplug CRC in hexadecimal. If the displayed CRC matches the CRC of the saved file, this provides assurance that the information in the two codeplugs is the same (with the exception of the settings that can be modified by the radio user after receiving the codeplug).
- **.efc**: This is the file extension for the OTA version of the Option Board Codeplug.

After Connect Plus CPS creates the file name for the saved OTA Option Board codeplug (.efc file extension), <u>do not edit or change the file name</u>! The file name must remain exactly as created by Connect Plus CPS, or the Network Manager will deny the file upload with a "File Name Error".

Caution! When editing an Option Board codeplug for OTA Codeplug File transfer, take great care if editing the Network IDs defined in the codeplug. <u>If the codeplug that is sent OTA has a different Network ID for the Option Board's currently selected zone, the Option Board will be unable to register back into the site and network after it updates to the new codeplug!</u>

If there is another Connect Plus zone in the same codeplug that is still configured with the Network ID that matches the XRC controller, then the radio user can resume operation on this network after manually selecting that zone. However, if there is no other zone in the codeplug with the same Network ID as the XRC controller, the Option Board Codeplug and Network Frequency File will have to be re-programmed before the radio can resume

using this network! The re-programming must be accomplished in the traditional manner, using Connect Plus CPS and a programming cable.

Locating the destination SU and initiating Option Board Codeplug File Transfer

After creating the saved codeplug for the destination SU, the steps for initiating the Codeplug File Transfer are as follows:

1. Place the saved codeplug in a known location on a PC that has the MOTOTRBO Connect Plus Network Manager software. This PC will be used to connect to the SU's registered site and to upload the saved file.

2. Because the saved codeplug must be uploaded to the specific Connect Plus site where the SU is currently registered, the Network Manager provides a "Find User" tool. Any network site can provide this information. After determining the SU's registered site, use the Network Manager to connect to that site. (Note: The registered site information returned by the "Find User" tool tells where the XRC thinks the SU is located, based on the SU's most recent registration. The XRC does not do a radio check to confirm communications with the SU. It is possible that the SU has faded since its last registration.)

3. Communicate with the radio user to determine if this is good time to initiate the OTA Codeplug Transfer. Do not upload the file until the following can be verified:

    a. Confirm that the radio user can tolerate a temporary interruption to service in order to receive the new codeplug. The best chance for successful transfer is when the radio user knows the codeplug transfer is imminent and does not attempt to initiate calls for a period of time.

        i. The best case scenario for interruption to service is thirty seconds (when the codeplug has 1 Option Board zone and the file needs to be sent just one time).

        ii. The worst case scenario for interruption to service is ten minutes (when the codeplug has 16 Option Board zones and the file needs to be sent three times).

        iii. The average interruption to service, which depends on the number of Option Board zones and RF conditions, will fall somewhere between these two extremes.

    b. Confirm that the radio is in a strong signal area (on a display radio, request the user to look at the number of bars on the signal strength icon).

    c. For a portable radio, confirm that the radio has an adequate battery charge (on a display radio, request the user to look at the number of lines on the battery strength icon).

4. After determining that this is a good time for the Codeplug File Transfer, use Network Manager to upload the Option Board Codeplug File. Connect to the SU's registered site. From the Main Menu, select *Site Control→Upload*, and then select the desired File Type. Press "File to Send", browse to the desired file, select the file, and press "Open". When the file name appears in the "File to Send" box, press "Upload".

5. Prior to uploading the file, the Network Manager will conduct several checks. If all checks are passed the file will be uploaded to the connected site. If any check fails, the file will not be uploaded, and a message will be provided to indicate why the Network Manager cannot proceed.

6. Before the Network Manager uploads the file, it provides a warning message stating that the Codeplug File Transfer can cause the radio user to miss calls. Acknowledge this message to proceed.

7. After successfully uploading the file, the XRC will begin the OTA file transfer as soon as possible, depending on several factors, such as the availability of resources, the number of queued data sessions, etc. The XRC does not store uploaded OTA Codeplug files to persistent memory. If the XRC reboots for any reason, it will be necessary to re-upload any undelivered OTA Codeplug file.

8. It is recommended to open the Network Manager's Real Time Display, and to watch for the Codeplug File Transfer to begin. Once the Codeplug File Transfer begins on the Real Time Display (RTD), it will continue for a period of time. How long depends on several factors. The System Administrator is encouraged to continue watching the RTD session until completion. When the session ends, the session "Shutdown Reason" in the RTD history panel will show whether or not the XRC considered the session to be successful.

9. If a session ends with an incomplete transfer, the XRC will not automatically re-initiate the session. The System Administrator must re-initiate the session by repeating the steps on this list.

The Option Board Codeplug File OTA Transfer Process

Once the Option Board Codeplug has been successfully uploaded to the controller, and when the controller has located an available repeater and timeslot, the OTA File Transfer process is as follows:

1. The SU is idle and monitoring the Control Chanel timeslot. It decodes a controller message assigning a trunk-to timeslot for Codeplug File Transfer.

2. On the trunk-to timeslot, the XRC and the SU exchange messages to confirm communication with one another, and the Option Board performs some checks. If communication cannot be established, or if the Option Board determines that the uploaded codeplug file does not have the correct Codeplug Version or Model information, or if the Option Board's current codeplug has the same CRC as the uploaded codeplug, the session will end prior to transferring packets. If this occurs, the RTD History Panel and the Event Log will contain information regarding the reason for the early termination.

3. If the file transfer process passes the preceding step, the controller begins to transmit file packets. The controller does not expect acknowledgement for each transmitted packet, but it does listen to the repeater uplink for messages from the destination Option Board.

4. As long as a display-capable SU remains on the assigned timeslot collecting packets, its display toggles between the Selected Contact Name and "File Transfer".

5. The collection of packets continues until one of the following occurs:

    a. The SU collects all file packets, verifies the file integrity, and transmits a message to inform the controller of successful file transfer. The SU will then upgrade to the new codeplug.

    b. The SU collects all file packets, but cannot verify the file integrity. The SU transmits a message to inform the controller that all packets were collected, but the file CRC could not be verified. In the case, the SU will discard the codeplug.

    c. Emergency Call is started on the SU's selected Group ID, Multigroup ID, or Emergency Revert Group ID. This will cause the controller to terminate the file transfer so that the SU can return to the Control Channel, and then join the Emergency Call.

    d. The radio user attempts to start a call. This will cause the radio to return to the Control Channel timeslot and transmit a Call Request. Upon receiving the Call Request, the XRC will end the Codeplug File Transfer.

    e. The SU's "Unconfirmed File Transfer Dwell Time" expires and the SU hasn't decoded a valid packet. This usually indicates the SU in is a fade condition, and it will cause the SU to return to

the Control Channel timeslot when the timer expires. The SU will subsequently enter Search if it doesn't hear anything from the Control Channel. The controller will continue to transmit file packets until one of the following occurs:

i. The SU re-registers with same site, or registers with different network site.

ii. The SU requests to start a call.

iii. Emergency Call is started on the SU's selected Group ID, Multigroup ID, or Emergency Revert Group ID.

iv. The controller completes the current file iteration, but doesn't decode any response from the destination SU.

6. The controller will transmit the Codeplug File for up to three consecutive iterations, but it won't start a new iteration unless it receives a "go ahead" from the Destination SU. The SU transmits the "go ahead" between iterations when it has decoded some, but not all, of the packets.

7. If the controller has transmitted three complete iterations of the Codeplug File, it will terminate the Codeplug File Transfer, regardless of whether the SU has collected all packets or not.

It is important to understand the following additional points about how Codeplug File Transfer operates:

- When the trunk-to session ends, for any reason, the controller will show the Shut Down Reason in the RTD History (if the RTD is open), and it will create an Event Log entry indicating whether the Codeplug File Transfer was successful. The controller's logged information can possibly be wrong. For example, if the Option Board transmits a message saying that it collected all packets and verified CRC, but the controller doesn't decode this message, the controller will log this as an "incomplete transfer", when it was actually successful.

- Once the trunk-to session ends, for any reason, the controller deletes the uploaded Codeplug File. The controller will not automatically initiate a new session. It is the responsibility of the System Administrator to initiate a new session by re-uploading the file.

- If the Option Board leaves a trunk-to session with an incomplete codeplug file, for any reason, the Option Board will not automatically re-join the same trunk-to session. Furthermore, any collected packets will not carry-over to the next codeplug file session. For the next codeplug file session, the Option Board starts collecting packets from scratch. This is different than how the Option Board operates for other OTA File Transfers.

- When the Option Board has received all file packets and verified CRC, it will automatically and immediately upgrade to the new codeplug. This will prolong the interruption to service by a few additional seconds. After upgrading to the new codeplug, the Option Board must re-register back into the network.

Note: When the Option Board upgrades to the new codeplug, the information in the new codeplug completely replaces the old codeplug. This means that codeplug edits performed by the radio user (such as contacts that were added via the menu) will be lost unless the same edits were also incorporated into the new codeplug.

Determining whether Codeplug File Transfer was successful

It is important for the System Administrator to determine if the Codeplug File transfer session was successful or not. If the session was unsuccessful, the system does not automatically re-initiate the Codeplug File Transfer. The System Administrator must re-initiate the transfer by re-uploading the desired Option Board Codeplug File.

The System Administrator can determine whether the transfer was successful by the following means:

1. Look at the Shut Down Reason in the Real Time Display History to see if the Codeplug File Transfer was successful.

2. Look at the Event Log entry to see if the Codeplug File Transfer was successful.

3. Communicate with the radio user to see if the CRC of the current Option Board codeplug matches the CRC of the uploaded codeplug file. Instruct the radio user to look on the menu under *Utilities→Radio Info→OB OTA CPcrc*. This menu option requires a display radio, and only appears when the Option Board's current codeplug was received over-the-air.

4. Communicate with the radio user to see if the Option Board is operating with its old or new settings. This option is available to both display and non-display radios.

5. As a last resort, there is the option to "read" the codeplug in the traditional manner using the programming cable and Connect Plus CPS. Then, compare the settings between the current codeplug and the uploaded codeplug.

2.8.7 OTA File Transfer Effects on Call Transmissions

Over-the-air File Transfer affects the SU's ability to receive calls.

- Option Board Codeplug File Transfer affects the destination unit's ability to receive calls.

- Option Board Firmware File Transfer and Network Frequency File Transfer can potentially affect all units on the site.

For this reason, it is important to understand how OTA File Transfer can impact the normal operation of the radio user:

Receiving Calls: Any time that the SU is acquiring file packets on a trunk-to timeslot, it will not see any call set-up messages that are transmitted on the Control Channel downlink. While this is true for any type of call that is received on a trunk-to timeslot, the duration of some Connect Plus File Transfers means that the SU can be "out of touch" with Control Channel messaging for an extended period of time. During this time, the SU will not receive calls.

Initiating Calls: OTA File Transfer will not prevent a SU from initiating a call. To initiate a voice call, the user must press and release the PTT button. This causes the radio to request a call on the selected Contact Name. If the radio was previously involved in a Codeplug File Transfer, it will also cause the XRC to end the file transfer session.

Even though the Connect Plus System allows call initiation during OTA File Transfer, it is important to realize that:

- The call set-up will not occur as quickly as it does when the SU is idle and monitoring the Control Channel timeslot.

- The target SU(s) might be engaged in the file transfer also. This is especially true if a Beaconed File Transfer is occurring on the site. If a target SU is involved in file transfer, it will not see the call set-up messages, and will not respond when a timeslot is assigned for the call.

- Initiating a call during Codeplug File Transfer will cause the file transfer session to end. The System Administrator will have to re-upload the file to start a new session. For this reason, it is important to communicate with the radio user prior to uploading the Codeplug File and to verify that the user can tolerate a temporary interruption to service.

2.8.8 Interaction of OTA File Transfer and Emergency Call

The Connect Plus SU allows the radio user to press the “Emergency On” button while the SU is receiving an OTA File Transfer on a trunk-to timeslot. This action will send the SU back to the Control Channel timeslot where it will transmit its Emergency Alert or Emergency Call Request (depending on Connect Plus CPS programming) on the Control Channel uplink.

Upon receiving any Emergency Call Request, the XRC performs some checks:

- If the Emergency Alert or Emergency Call is sent on the Selected Group ID, Multigroup ID, or Emergency Revert Group of any SU currently involved in OTA Option Board Codeplug File Transfer, the XRC will end the File Transfer session.

- The XRC checks to see if there is any Beaconed File Transfer (Option Board Firmware File or Network Frequency File) currently in progress. If so, the controller terminates the File Transfer. The XRC takes this action because it does not know which specific SUs are listening to the Beaconed File Transfer. When the controller terminates the File Transfer, all of the SUs that were involved in the transfer return to the Control Channel timeslot. This allows the SUs to see the call set-up messages on the Control Channel downlink and respond to the Emergency Alert or Emergency Call if it happens to be on a Group ID of interest.

The XRC does not automatically resume the interrupted OTA File Transfer when the Emergency Alert or Emergency Call ends. If the Network Administrator wishes to re-start the OTA File Transfer, he/she must re-upload the desired Connect Plus OTA file.

2.8.9 Selecting Optimal Conditions for OTA File Transfer

While OTA File Transfer provides many potential benefits to Connect Plus network management, it is extremely important for the Radio System Administrator to understand how it affects system and radio operation, so that he/she can select the optimal conditions for scheduling OTA File Transfer.

To provide the best opportunity for successful file transfer, and to minimize impact to normal system communications, OTA file transfers should be scheduled to occur during the trunking system’s quiet hours. If possible, the radio should be placed in a stationary location with good reception and reliable power. Do not attempt to program the radio with MOTOTRBO CPS or Connect Plus CPS during an ongoing OTA file transfer.

A previous section discussed the optimal conditions for conducting a successful Codeplug File Transfer. As discussed in that section, it is important to discuss an impending Codeplug File Transfer with the radio user prior to uploading the Codeplug File.

The following sections are primarily intended to describe the optimal conditions for Beaconed File Transfers (Option Board Codeplug File and Network Frequency File).

Recommendations for the radio user:

- Leave radio on.

- For portable radio, utilize a fresh battery, or place radio in battery charger or use a “battery eliminator”.
- Verify radio is in a good coverage location.
- If possible, do not pick-up the radio or make calls during OTA File Transfer.

Recommendations for the Network Administrator:

- When selecting the dedicated repeater and timeslot, consider the following:
  - Select a clear frequency that is not prone to interference.
  - If possible, select a repeater that will not have to send Base Station Identification during the File Transfer process.
- Dedicate the repeater timeslot for as long as possible. The more times the repeater sends the file, the greater the chance the file will be acquired by the largest possible number of radios.
- “Time to Begin” should be set for a date and time where the system is as quiet as possible. “Off-hours” transfers provide the best opportunity for success.

2.8.10 Assigning Repeater for OTA File Transfer

When using a dedicated channel for unconfirmed file transfer, it is recommended that “Time to Dedicate” should be set at least long enough so that the controller can send (at a minimum) three completion iterations of the file.

For this reason, it is helpful to know how long it takes the controller to transmit a single iteration of the file. Because this is related to the file size, it will take much longer to transmit a Connect Plus Option Board firmware file than a Network Frequency File.

The following equations can be used to make a rough calculation of how long it will take the controller to transmit a single iteration of a file in unconfirmed file transfer.

File size in bytes/180 = number seconds to send the file

Number of seconds to send file/60 = number of minutes to send the file

When the “Time to Dedicate Repeater” expires, the controller will complete the current file iteration prior to ending the dedicated channel transfer.

2.8.11 Special Considerations for the Network Frequency File

Special considerations for the Network Frequency File in OTA file transfer include the following:

- The Network Frequency File version number (which determines whether or not the SU will acquire an updated Frequency File OTA) is set by the individual that creates the Network Frequency File (using Connect Plus CPS). It is recommended that a single individual, such as the Network Administrator, has the responsibility for creating the Network Frequency File and managing version numbers.

- When setting a dedicated Repeater & Timeslot for OTA Network Frequency File transfer, Connect Plus recommends that the programmer configure Timeslot 2 of the Control Channel repeater as the dedicated repeater and slot.

For further recommendations and other important information about the Network Frequency File, see the section on Network Frequency File.

2.8.12 Radio User Request to Re-join OTA File Transfer

The Connect Plus Utilities Menu can be used to view its (Pending) “Updates”. The “Updates” option applies to the Option Board Firmware File and the Network Frequency File only. A “pending update” is any file that the SU is aware of, and needs, but hasn’t collected all file packets. It is also any file where the SU has received all packets, but has not yet upgraded to the new file. The “pending updates” option shows the file type and (when there is a pending file) the percentage of packets collected so far. When there is a pending file, but the Option Board has not collected all file packets, the Menu allows the radio user to request that the SU re-join an ongoing Beaconed File Transfer, even though the “File Transfer Attempt Interval” has not expired.

2.9 Busy Queue

If subscriber makes a Call Request requiring a trunk-to timeslot, the Call Request will be granted if a timeslot is available. Otherwise, the controller shall place the call in the Busy Queue and send the source radio a Busy Queue Grant on the Control Channel timeslot. The controller shall periodically re-send the Busy Queue Grant as long as the call remains in the Busy Queue. The Busy Queue Grant allows the source radio to know that its requested call is still in the queue. If the queued call is a Group Call, the Busy Queue grant also has the effect of inhibiting call requests by other radios on the same Group ID. When a trunk-to timeslot becomes available, the calls are assigned from the Busy Queue according to the following rules:

- If requested, the Emergency Call[18] is assigned to the trunk-to timeslot.
- If requested, the Emergency Location Update[19] is assigned to the trunk-to timeslot.
- The highest non-emergency priority call is assigned to the trunk-to timeslot.
- For calls of equal priority, voice calls have priority over data calls.
- For voice calls of equal priority, calls are assigned “first in, first out”.
- For data calls of equal priority, calls are assigned “first in, first out”.

When the Busy Queue is clear of all Emergency Calls and Emergency Location Updates, non-emergency calls are assigned from the queue according to the configurable priority level of the IDs involved in the call. Every Connect Plus User Record (both the Unit Record and the Group Record) has a programmable priority level, with 2 being the highest programmable priority level and 8 being the lowest programmable priority level. When the controller assigns calls from the Busy Queue, it does so according to the priority levels of the IDs contained in the

[18] Emergency Calls are placed on “Top of Queue”. When multiple Emergency Calls are in the Busy Queue, they are assigned to available timeslots on a “first in, first out basis”.

[19] When multiple Emergency Location Updates are in the Busy Queue, they are assigned to available timeslots on a “first in, first out basis”.

Call Request. Every Call Request has a Source ID and a Destination ID. The call is assigned from the Busy Queue according to the higher of the two priorities. Site All Call requests are prioritized according to the priority of the Source ID only. A Network Wide All Call request (which can only be made by a non-radio device such as a digital wireline console) is handled the same as a Site All Call request.

It should be noted that for non-emergency calls, a source SU can "cancel" its Busy Queue status, which allows the radio user to initiate a different type of call. Once a call request has been placed in the Busy Queue, the radio will stay in "Busy" mode until the call is assigned, or until the user presses the Busy Queue Cancellation button (if programmed by the radio dealer or system administrator). If the user does not "cancel" the call request, it is likely that such call request will eventually be granted a timeslot. However, if the radio user doesn't initiate the call, the granted call will probably will be processed as a brief, failed call, but the user will most likely not be aware of such event.

The Busy Queue cancellation button does not apply to Emergency Calls. Once accepted to the Busy Queue, the Emergency Call remains in the queue until assigned to a timeslot. The source SU will respond to the call assignment. If the emergency condition no longer exists, the radio user should verbally explain this, and then allow the Emergency Call to expire.

2.10 Network Frequency File

The Connect Plus subscriber radio stores frequency information in the Network Frequency File. This file, which is created with Connect Plus CPS, must contain the Network ID, a customer-settable version number, and the following information about each repeater in the Connect Plus network.

- Which site the repeater is located at.
- The repeater's Radio ID (1-15). In the Connect Plus system, this equates to the channel (repeater) number.
- SU TX (Repeater RX) Frequency
- SU RX (Repeater TX) Frequency
- The repeater's Color Code
- A checkbox to indicate if the repeater can operate as the Control Channel. Connect Plus Option Board CPS allows up to four repeaters to be checked as Control Channel repeaters, but only one of these will be active at any given time as the site's Control Channel. When active as the Control Channel repeater, Timeslot 1 is used for Control Channel messages and Timeslot 2 is available for call assignments. When not active as the Control Channel repeater, both timeslots are available for call assignments. For more information on how the XRC determines which repeater will be the active Control Channel, see the Section, "Control Channel Rollover".

The Connect Plus radio can be configured with up to sixteen Network IDs. For every network that will be used by the radio, the radio must also be programmed with a Network Frequency File that has a matching Network ID. The radio only uses one of these networks (and one Network Frequency File) at a time, depending on which Connect Plus zone is currently selected. For important information about how to configure a Connect Plus radio with multiple Network IDs (and multiple Network Frequency Files), see the section "Network ID."

2.10.1 Importance of Network Frequency File

The Network Frequency File plays a crucial role in both trunking and roaming. When the Connect Plus is idle and monitoring the control channel, it continually looks for channel assignments on the control channel downlink. Among other things, these messages are used to move radios to trunk-to timeslots for Connect Plus calls. The message does not give the actual repeater frequency, because this is too long to be efficiently communicated in a short message. Instead, it gives the Repeater Radio ID (1-15) as programmed with Connect Plus CPS, as well as the assigned timeslot (1 or 2). To determine which frequency it should use, the Connect Plus SU looks up the given Repeater Radio ID on its Network Frequency File table for the registered site. This tells the SU which frequency pair and Color Code it should use when moving to the assigned repeater and timeslot. For information on how the Connect Plus SU uses the Network Frequency File when searching for service (roaming between sites), see the "Frequencies Searched" section.

For proper operation, the Connect Plus SU's Network Frequency File must match the actual network configuration at all times. It is recommended that a single individual, such as the Network Administrator, have the responsibility for creating the Network Frequency File and managing version numbers. There are two ways the SU receives the Network Frequency File.

- During initial Connect Plus CPS programming, the SU should be loaded with the most recent Network Frequency File.
- If the Network Frequency File is changed after initial programming, there are two ways to update the file:
    - Load the updated file via the programming cable and Connect Plus CPS.

Update the radios via an Over-the-air File (OTA) Transfer. For more information about how the Network Frequency File is sent over-the-air, see the "Connect Plus Over-The-Air File Transfer", and specifically the "Special Considerations for the Network Frequency File" section.

2.10.2 Changes Impacting the Frequency File

Sometimes it is necessary to make changes to frequency information in the Connect Plus network. This occurs when frequency information changes, repeaters are added or removed, sites are added or removed, Control Channel information changes, Color Code information changes, etc. When this occurs, the Network Frequency File will have to be updated with the new information (and issued a higher version number). When changes such as these occur, the order that things happen is very important. For example, all radios should have the frequency information for a new repeater (via an updated Network Frequency File) before the repeater is brought on line. Recommendations are provided for some of the most common scenarios:

The recommended procedure for <u>adding a new repeater to a site</u> is as follows:

- Determine the frequency information, color code setting, and MOTOTRBO Radio ID (1-15) for the new repeater.
- Update the Network Frequency File with this information and increment the Network Frequency File version number.
- Upload the updated Network Frequency File to the site(s) and begin OTA File Transfer.
- Allow sufficient time for deployed radios to update to the new Network Frequency File.

- Configure and align the new repeater and connect it to the Ethernet switch shared with the trunking controller. The repeater will establish a link with the controller, after which the controller will begin assigning calls to the new repeater.

The recommended procedure for changing the frequency or Color Code configuration of an existing non-Control Channel repeater is as follows:

- Determine which information needs to be modified.
- Update the Network Frequency File with this information and increment the Network Frequency File version number.
- Prior to uploading the Network Frequency File to the network, disable the affected repeater to keep the controller from using it as a trunk-to resource. This can be done by physically disconnecting the repeater from the Ethernet switch. This will terminate communications with the controller, causing the controller to quit assigning calls to the repeater.
- Upload the updated Network Frequency File to the site(s) and begin OTA File Transfer.
- Allow sufficient time for deployed radios to update to the new Network Frequency File.
- Change the repeater configuration to match the revised information in the Network Frequency File, and connect the repeater to the Ethernet switch shared with the trunking controller. The repeater will establish a link with the controller, after which the controller will begin assigning calls to the repeater.

The recommended procedure for adding a new site to the network is as follows:

- Determine the Site Number, Repeater Radio IDs (1-15), frequency information, frequencies, repeater color codes, and control channel information for the new site.
- Update the Network Frequency File with this information and increment the Network Frequency File version number.
- Upload the updated Network Frequency File to the network and begin OTA File Transfer.
- Allow sufficient time for deployed radios to update to the new Network Frequency File.
- Configure the controller and repeaters for the new site. Connect the repeaters to the controller via the Ethernet switch.
- Update the network multi-site information (in the other Connect Plus sites) to include the Site Number and IP address of the new controller.
- In the RF-adjacent sites, add the new site number to the Neighbor Site List. This allows the RF-adjacent controllers to beacon the new Site Number in the Neighbor Site message.
- When the Option Board has the updated Network Frequency File, and has collected the new Neighbor List information, it will be ready to use the new site.

2.11 Controller Multi-Site Features

Multi-Site operation is available as a purchasable, factory-enabled permission in the Connect Plus controller. It can be activated at time of initial purchase, or remotely activated at a later date. When enabled, the controller activates certain parameters pertaining to multi-site operation that are not available single-site operation. The most of important of these settings is the ability to configure a list of networked sites.

2.11.1 Registration & De-Registration in a Multi-Site Environment

When a Connect Plus subscriber registers or de-registers with one of the site controllers, the controller forwards this information to all other site controllers. This allows all controllers to have the same information about which IDs are (or are not) currently registered into the network.

2.11.2 Call Processing & Set-up in a Multi-Site Environment

When the controller receives a Call Request, it must know if the Destination ID is registered into the network, and – if so – at which site(s). The controller has this information because a registration or de-registration received by any site controller is forwarded to all other site controllers.

It's quite possible that multiple controllers will have a role in Connect Plus call set-up. Calls to an individual ID can involve up to two sites, the source site and the destination site. Calls to Group IDs will involve every network site where the Group ID is presently registered. Multi-site call set-up is initiated via TCP/IP control messages that are exchanged between the involved sites.

Depending on resource availability, it is possible that the multi-site call may be placed on the air at some sites and placed in Busy Queue at other sites. If the call transmission is still in-progress when a voice channel becomes available, the queued call will be assigned from the Busy Queue. (Each call is assigned from the Busy Queue according to the configured priority level on the call initiator's user record.) Radios at that site which are not already engaged in a call will hear the remainder of the active call transmission as late-joiners. If the call transmission ends before a voice channel becomes available, it will be removed from the Busy Queue.

A site that receives a voice transmission must duplicate the received UDP/IP voice packets and forward them to every network site where the Destination ID is currently registered. It is possible that multiple radios involved in the same call (but located at different sites) will begin to transmit at the same time, or at nearly the same time. For this reason, the controllers involved in a multi-site voice call follow a key-up arbitration procedure. The arbitration process necessitates a brief (configurable) delay before a controller forwards received voice packets to one of its connected repeaters for OTA transmission, but it greatly increases the chances that the same audio will be heard at each participating site.

When a controller has an undelivered text message for an SU, and the controller learns via network messaging that the SU has registered to a different site, the controller will forward the text message to the SU's new site. The controller at the new site will attempt delivery at the earliest opportunity.

When a controller has Location Request for an SU, and the controller learns via network messaging that the SU has registered to a different site, the controller will forward the Location Request to the SU's new site. For a single request, the new site will transmit the request at the earliest opportunity. For a periodic request, the new site will transmit the first request at the earliest opportunity, and then repeat the request at the requested interval.

2.12 Roam (Site Search) in Connect Plus System

The Connect Plus subscriber unit will automatically roam (search for service), and upon locating an acceptable site, will automatically request registration with the Connect Plus site.

2.12.1 Events that Initiate Site Search

The following events cause the subscriber to initiate the search process:

- Radio is powered-up in a Connect Plus zone.
- Radio user selects a Connect Plus zone (or changes from one Connect Plus zone to a different Connect Plus zone).
- Radio is registered to a Connect Plus site, but does not decode a Control Channel message before its programmable “CSBK Roam Delay Time” expires. This can occur for a number of reasons, such as (1) radio is in a low-signal location, (2) site is doing Control Channel Rollover, and (3) site equipment is experiencing problems.
- Radio is registered to a Connect Plus site, but RSSI from the Control Channel repeater is at or below the programmable “RSSI Minimum” threshold. This causes the SU to start its programmable, “RSSI Roam Delay Timer”. If this timer expires and the Control Channel RSSI has not risen above the “RSSI Minimum”, the SU initiates the search process.
- When the Connect Plus radio is operating in Auto Fallback mode, the radio periodically verifies that it is still hearing the Fallback Channel. If the radio cannot verify that it is still hearing the Fallback Channel within an expected period of time, the radio will return to Search mode.

2.12.2 Conditions for Withholding Search

The Connect Plus SU will not initiate Search in the following circumstances:

- The Connect Plus SU will not initiate Search while it is attempting to initiate a call on the Control Channel timeslot. If RF conditions are poor, it is possible that the call attempt will fail – after which the SU may initiate search for one of the previously described reasons.
- The Connect Plus SU will not initiate Search while it is Busy Queue Wait State on the Control Channel timeslot. The SU’s (non-configurable) Busy Queue Wait timer must first expire.
- The SU will not initiate Search while participating in a call-in-progress on a trunk-to timeslot. If the SU loses signal from the trunk-to timeslot, it will return to the Control Channel timeslot. If the Control Channel signal does meet the previously discussed requirements, the radio will initiate Search.

2.12.3 Frequencies Searched

The Connect Plus SU stores Control Channel and Trunk Channel frequency information in the Network Frequency File. The Network Frequency File is used both for single-site and multi-site networks. For general

information about the file and how it is created, see the " Network Frequency File" section. This section will discuss its role in search process only. The Connect Plus SU stores Auto Fallback Channel information (if so configured) in its Connect Plus codeplug.

A Connect Plus SU can be programmed with Network Frequency Files for up to sixteen different Network IDs. However, the Connect Plus radio only loads one of these Network Frequency Files at a time. The Connect Plus Option Board loads the Network Frequency File that matches the Network ID for the currently selected Connect Plus zone. The Connect Plus SU does not automatically roam between different networks while selected to a single Connect Plus zone. If the radio user wants the Connect Plus radio to search a different network, he/she must select the Connect Plus zone that is configured for that network. Upon changing zones, the Connect Plus radio loads the Frequency File with the Network ID that matches the selected zone, and begins searching frequencies from that Network Frequency File. It will only search frequencies from this Network Frequency File as long as it remains selected to the same zone.

When the SU is searching for service, it only searches frequencies that are configured as Control Channels or Fallback Channel for the site that is being searched. The general rule is that the Connect Plus SU searches all of a site's possible Control Channels (as flagged in the Network Frequency File) before it searches the configured Fallback Channel. For a detailed discussion of Fallback Search, see section 4.6.5. If the SU does not detect either an active Control Channel or an active Fallback Channel, the SU proceeds to search the next site on its list. The order that sites are searched depends on several variables. This includes the following:

- **Preferred Site:** For each Connect Plus zone, the SU is configured with a "Preferred Site". The Control Channel(s) for the "preferred site" receive a heavier weighting in the search algorithm (meaning that it is searched more frequently). It is important to note that the SU will always register on the Preferred Site or Preferred Last Register site (if the option is enabled) even if the SU is within coverage of another site with better signal. The Preferred Site is searched in the following circumstances:
  - After initial Connect Plus CPS programming, it is the first site searched when the user first powers-up in (or selects) that Connect Plus zone.
  - It remains the first site searched (power up, zone selection, losing signal from a site, etc), if "Preferred Last Registered" has not been enabled via Connect Plus CPS programming for that Connect Plus zone.
  - Even if "Preferred Last Registered" Site has been enabled via Connect Plus CPS programming for that Connect Plus zone, the "Preferred Site" is searched more frequently than other sites (except for the Last Registered site).

- **Last Registered:** The Connect Plus SU stores the Site Number where it last successfully registered. This information is stored in persistent memory, so that it will be maintained through a power cycle. This Last Registered Site receives a heavier weighting in the search algorithm. This weighting can be increased even further by enabling "Prefer Last Registered" via Connect Plus CPS (a programmable option per Connect Plus zone). When "Prefer Last Registered" is enabled, the Last Registered Site becomes the first site searched upon power up, zone selection, losing signal from a site, etc. Of course, this assumes that radio has successfully registered somewhere. If not, the "Preferred Site" is searched.

- **Neighbor List Collection:** When a Connect Plus SU is registered to a site, it collects the "Neighbor List" that is transmitted by the site's control channel. The Neighbor List consists of up to 5 site numbers for sites that are RF-adjacent to the site transmitting the Neighbor List. This Neighbor List is configured by using the Network Manager Software. When a Connect Plus SU loses signal from a site, it first searches the "Preferred" or "Last Registered" site (as determined through Connect Plus CPS programming). If an acceptable signal is not found, the SU proceeds to search the Control Channels of the most recently collected Neighbor List. In doing so, all Neighbor List sites will be searched and the *strongest* RSSI site will be selected provided the signal is at least at the "RSSI Preferred" level. The Connect Plus SU can store Neighbor Lists collected from up to 10 different Connect Plus sites. The lists are searched in "last

collected, first searched order". If the SU should ever collect Neighbor Lists from more than 10 different sites, the oldest Neighbor List will "fall out" to make room for the most-recently collected Neighbor List. An example of a Neighbor List configuration is shown in Figure 2-7.

- **Other Sites pulled from the Network Frequency File:** As the Connect Plus SU searches for service, it will periodically search the Control Channel(s) for other Connect Plus sites pulled from the Network Frequency File. If a search goes on long enough (without locating an acceptable site and signal), the SU will eventually search every Control Channel for every site in the Connect Plus network.

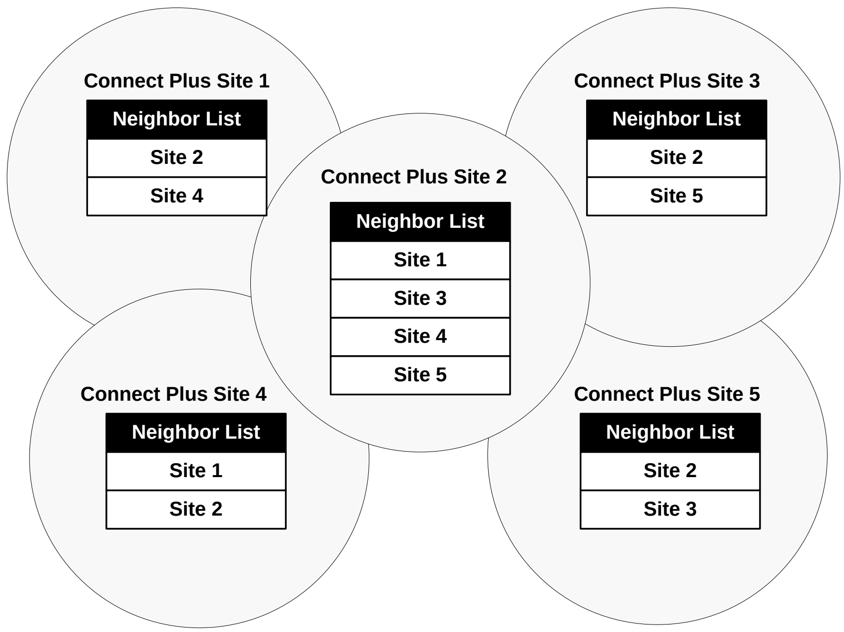


Figure 2-7 Connect Plus Neighbor List Example

2.12.4 Qualifying Searched Sites

As the Connect Plus SU moves through the Control Channel frequencies on its search list, it listens to each frequency for the "Roam Dwell Time" as configured via Connect Plus CPS programming. This setting is configurable per Connect Plus zone. Because Control Channels transmit continuously, this is a fairly short timer (240 to 1200 ms). If digital signaling is detected, the radio waits an additional time to identify the site and network (via Connect Plus control channel messaging) and to measure RSSI. If this time expires and the radio has not detected digital signaling, it then proceeds to search the next frequency on the list. It should be noted that the IP Site Connect Beacon message is not used in Connect Plus. The IP Site Beacon Duration should be set to "Disabled" in the CPS codeplug of all Connect Plus repeaters.

If digital signaling is detected, the SU will wait on the frequency long enough to determine the Network ID and the Site Number of the Control Channel it is hearing. This information is sent every 120ms on the Control Channel downlink. If the Network ID transmitted by the Control Channel agrees with the Network ID programmed into the SU via Connect Plus CPS, the SU proceeds to measure the Control Channel RSSI. If the RSSI is equal to or greater than the "Preferred RSSI" as programmed for the Connect Plus zone via Connect Plus CPS, the SU

operation depends on whether the radio is searching its most recently collected Neighbor List, and whether it still has other sites from that list to evaluate. If so, the SU remembers the detected RSSI level and proceeds to search the next Neighbor Site. If the SU is not searching its most recently collected Neighbor List, or if the SU has already completed its Neighbor List search and selected the strongest available site, the radio will transmit a registration request to the site controller on the Control Channel uplink. Because the Network ID and RSSI are important parts of qualifying a site, they are discussed in greater detail in the sections that follow.

If the Connect Plus SU has been configured to search Auto Fallback Channels (in addition to Control Channels), the amount of time that the SU dwells on the Auto Fallback frequency depends on several factors. Most importantly, the Auto Fallback Channel search increases the overall site search time significantly, because by default the dwell time is 5 seconds *per site* for non-continuous beacon channels. As an example, on a 31-site system with non-continuous Auto Fallback Channels at each site, the site search *increases* by 150 seconds (worst case). For a detailed discussion of Fallback Search, see section 4.6.5.

2.12.5 Roam Request

"Roam Request" can be enabled via a programmable Connect Plus button press. Roam Request allows the radio user to request the radio to enter "Search" mode and look for another network site, even when the signal from the currently registered site is acceptable according to the currently programmed Roam parameters. When Roam Request is activated, the SU will search all possible sites until an acceptable site is found, which may end up being the current site, if no other sites with or above "Preferred RSSI" are detected.

2.12.6 Radio Operation during Search

A Connect Plus radio cannot make and receive calls unless it registered to a Connect Plus site. When the Connect Plus SU is searching for service, it is not registered with any Connect Plus site. If the user attempts to initiate a non-emergency call by pressing PTT, the radio will give a denial tone. If the user attempts to initiate a non-emergency call via the Menu, the display will show "Not Registered".

The Connect Plus SU does allow the radio user to press the "Emergency On" button while the radio is Searching. Although the SU will not be able to immediately send the Emergency Alert or Emergency Call Request in this scenario, it will automate the process of locating and registering with a Connect Plus site, after which the SU will immediately and automatically transmit the Emergency Alert or Emergency Call Request. (Whether the radio sends an Emergency Alert or Emergency Call request depends on Connect Plus CPS programming for the selected zone.) If the radio user changes his/her mind about the Emergency before the SU locates a site, registers, and sends the Emergency Alert or Emergency Call request, he/she should press the "Emergency Off" button to cancel. Once the radio registers with a site and sends the Emergency Alert or Emergency Call request, the user will not be able to cancel by pressing "Emergency Off". If the radio starts an Emergency Call, when the call is assigned to a trunk-to timeslot, the radio user should verbally explain that there is not an actual emergency, and then allow the Emergency Call to expire. If the radio sends an Emergency Alert, the user can explain that the situation is not a real emergency when another radio user or console operator responds to the Emergency Alert.

While the Connect Plus SU is searching, the top LED blinks yellow in a "double flash" pattern.

While the Connect Plus SU is searching, display-enabled radios activate the Roaming icon and display the word "Searching".

2.12.7 Indications of Successful Registration

When a Connect Plus radio successfully registers with a site, it sounds a short registration beep and briefly displays the registered Site Number in the radio display. The LED flashes green while the radio is monitoring the

Control Channel downlink. If not currently engaged in another Menu Display, the radio display shows the “Contact Name” for the selected channel knob position (portable) or rocker knob position (mobile).

After completing registration with a site, the Connect Plus SU does not continue to display the registered site number. However, selecting the *Utilities→Radio info→Site Number* menu option causes a display-equipped radio show the registered site number (or “Not Registered”, if the SU is searching for service).

If the Connect Plus SU acquires a Fallback Channel as a result of the search process, there is no registration message exchange (and, therefore, no registration beep). However, the radio will provide a periodic, intermittent tone as long as it remains on the Fallback Channel. For a detailed discussion of Fallback Search, see section 4.6.5.

2.12.8 Reacquiring the Same Site after Period of Fade

When the radio loses acceptable signal from its current site and begins searching, a countdown timer is set to the value configured in the “Reacquire Time” setting. This is a programmable Zone parameter with Connect Plus CPS. If during the search process the radio again finds the site it just lost and this timer has not expired and the radio has not attempted to register at another site, the radio returns to the registered state without transmitting a registration request (or sounding the registration beep). If the Reacquire Time has expired, the radio must complete a normal registration before it can use the site. This feature can help reduce registration traffic on the Control Channel and extend portable battery life.

2.12.9 Site Restriction by Subscriber Unit ID

Connect Plus provides the ability to configure, via the Connect Plus Network Manager, which network sites can (and cannot) be used by the Connect Plus Subscriber Radio. The Site Restriction feature is useful for cases when a Connect Plus SU should not be allowed to use certain network sites (such as when the disallowed sites are under different ownership.) The feature provides the ability to update the list of allowed/disallowed sites via the Network Manager without having to re-program the Subscriber Unit. The terms “restricted site” and “disallowed site” are used interchangeably.

Beginning with Release 1.7 (R2.6.0), the SU Site Restriction feature is configured on the Site Access and Permanent Registration (SAPR) screen in the MOTOTRBO Connect Plus Network Manager software application (when connected to an XRC Controller site) or in the MOTOTRBO Connect Plus Configuration Tool application (when connected to a XRT Gateway site). Because the SU Site Restriction information is stored behind the scenes as part of the user database, the SU Site Restriction settings configured via the SAPR screen are automatically shared with all other sites in the same Connect Plus network. It is not necessary to configure the same information at multiple sites. To the contrary, it is recommended to make all SAPR screen edits at only one designated network site. The SU Site Restriction settings are no longer visible when viewing a Unit record in the User Registration screen. Because the User Registration Screen and the Site Access and Permanent Registration (SAPR) Screen are both capable of modifying information in the Connect Plus user database, it is not recommended to open both screens at the same time.

The Site Access and Permanent Registration screen provides two ways to configure restricted sites[20] for subscriber units:

- From the site perspective view, the application user can add or remove one or more radios from the site’s list of restricted radios. Any valid subscriber that is not on the restricted list is allowed to use the site.

[20] By default, all radios are allowed to use all sites.

- From the SU perspective view, the application user can add or remove one or more restricted sites for a specific subscriber radio.

A Connect Plus SU must make at least one attempt to register with a disallowed site in order to learn that it is not allowed to use the site. When the XRC receives a registration request from a Connect Plus SU, its first check is whether the radio's UID and Group ID exist in the controller's database. If not, the controller sends a message to disable the SU. If the UID and Group ID exist in the database, the next check is to see whether the present site is allowed or disallowed for the registering SU. If disallowed, the XRC responds to the registration by informing the SU that it is attempting to register on a disallowed site. When the Connect Plus SU receives this response, it provides a special tone to inform the user that the site is not allowed. Display radios also briefly show a message that "Site 'x' is Not Allowed". Then, the Connect Plus SU goes back into Search to look for another site. The Option Board places the disallowed site on an internal blacklist. As long as the site remains on its internal blacklist, the Connect Plus SU will not make any further attempts to register with the disallowed site.

By design, the SU keeps its list of disallowed sites in volatile memory only. The SU clears the list of disallowed sites upon any event that causes an Option Board reset. This includes power cycling the radio, programming the radio or Option Board, etc. After the Option Board clears its internal site blacklist, it will once again attempt to register with any network site. If the user record still shows that the site is "disallowed", the process starts over. However, if the user record has been updated so that the site is now listed as an "allowed site", the registration will be allowed, provided that the radio passes all of the normal registration checks.

It is important to understand the following about how the Site Restriction feature works in Connect Plus:

1. If the Connect Plus SU is currently registered to a site, and the SAPR screen is edited to make it a disallowed site for that radio, the SU will remain registered to the site until its next registration attempt. Any event that normally causes a new Connect Plus registration (such as the user changing the selected Talk Group), will cause the SU to be informed that the site is now disallowed.

2. If the Connect Plus SU has been informed, via the registration response, that a site is disallowed, and then the System Administrator subsequently changes the user record to make it an allowed site, the Connect Plus SU will still not attempt to use the site until the internal site blacklist is cleared. The following actions will clear the blacklist; cycling power on the SU, replacing the battery, programming the radio or Option Board, etc.

3. If the controller sees that a SU is attempting to register on a disallowed site, it informs the SU of this in its registration response. The controller does not perform the other database checks for the SU (such as the ESN check). These checks are only performed and enforced when the XRC receiving the registration request is an allowed site for the SU.

4. It is important to understand the interaction between Connect Plus Site Restriction and other Connect Plus features that limit Roaming:

    a. **Disable Roam checkbox in Connect Plus CPS**: Checking the "Disable Roam" checkbox in Connect Plus CPS tells the SU that it can only Search its "Preferred Site" number (also configured with Connect Plus CPS) while selected to that Connect Plus zone. If the Connect Plus SU has been programmed in this manner, do not restrict this same site number for this SU when configuring the Network Manager SAPR screen. Doing so would prevent the SU from using any network site.

    b. **Site Lock button**: Connect Plus CPS provides the ability to configure a Site Lock button. When the SU is registered to a site, and Site Lock is engaged, the SU will not search any other site number until Site Lock is disengaged. If a SU is registered to a site, and then the same site is configured as disallowed on the SU's site list in the Network Manager SAPR screen, the SU will discover this on its next registration attempt with the site (such as when the radio user selects a

different Talk Group). If this were to occur, the radio would then be “locked” to a disallowed site (and therefore not using any site) until the Site Lock button is disengaged. Power cycling the radio also disengages Site Lock.

5. It is important to understand the interaction between Connect Plus Site Restriction and Emergency. If a radio is searching with “Emergency Pending”, it must first successfully register with a site before it can transmit its Emergency Request. The SU cannot register (or transmit an Emergency Request) to a disallowed site. The recommendation is as follows: If a Connect Plus radio is enabled for “Emergency Init” on its Call Privileges in the XRC user database, it should also be enabled for all network sites on its Site Privileges.

2.12.10 Site Restriction by Talk Group ID

Connect Plus provides the ability to configure, via the Network Manager and XRT Configuration Tool applications, which network sites can (and cannot) be used by specific Talk Group IDs. The Site Restriction by Talk Group feature is useful for cases when a Talk Group ID should not be allowed to use certain network sites (such as when the disallowed sites are under different ownership or when they have limited RF resources.) The feature provides the ability to update the list of disallowed sites for each Talk Group (and/or the list of disallowed Talk Groups for each site) via the application without having to re-program the subscriber radios. The terms “restricted site” and “disallowed site” are used interchangeably. The Site Restriction by Talk Group Feature should not be used to prevent a subscriber radio from using a specific site no matter which Talk Group is currently selected. In that case, use the Site Restriction by Subscriber Unit ID feature as discussed in section “*Site Restriction by Subscriber Unit ID*”.

The Site Restriction by Talk Group feature is configured on the Site Access and Permanent Registration (SAPR) screen in the MOTOTRBO Connect Plus Network Manager software application (when connected to an XRC Controller site) or in the MOTOTRBO Connect Plus Configuration Tool application (when connected to a XRT Gateway site). Because the Site Restriction by Talk Group information is stored behind the scenes as part of the user database, the Group Restriction settings configured via the SAPR screen are automatically shared with all other sites in the same Connect Plus network. It is not necessary to configure the same information at multiple sites. To the contrary, it is recommended to make all SAPR screen edits at only one designated network site. The Site Restriction by Talk Group settings are not visible when viewing a Group record in the User Registration screen. Because the User Registration Screen and the Site Access and Permanent Registration (SAPR) Screen are both capable of modifying information in the Connect Plus user database, it is not recommended to open both screens at the same time.

The Site Access and Permanent Registration screen provides two ways to configure restricted sites[21] for Talk Group IDs:

- From the site perspective view, the application user can add or remove one or more Talk Group IDs from the site’s list of restricted Groups. Any valid Group that is not on the restricted list is allowed to use the site.

- From the Group perspective view, the application user can add or remove one or more restricted sites for a specific Talk Group ID.

A Connect Plus radio must decode a special controller message in order to learn that it is not allowed to use a specific Talk Group at a specific site. Most often, the SU decodes this message when it attempts to register on the site while selected to the restricted Talk Group. The controller responds to the registration attempt with a message informing the registering radio that the Talk Group is not allowed at the site. The message will also be decoded by other radios that are monitoring the Control Channel at the time. Additionally, if radios are currently

[21] By default, all Talk Groups are allowed to use all sites.

registered to the site on the Talk Group when the group record configuration status is changed from “allowed” to “disallowed”, the controller makes a best effort to inform the currently registered population so that radios currently registered to the “disallowed” group will roam away from the site.

When the radio decodes the message that it is attempting to register on (or is currently registered on) a restricted Group for the site, the radio provides a tone to alert the radio user. Display radios also briefly show a message to inform the user that the Group cannot be used. Then, the radio goes back into Search to look for another site. The radio places the disallowed site and group combination on an internal blacklist. As long as the site and group combination remains on its internal blacklist, the Connect Plus SU will not make any further attempts to register on the disallowed site while selected to the blacklisted Group. It is important to note, that this applies only to the specific Talk Group ID indicated in the controller message. It is possible that the radio has been programmed with other Groups that are allowed Groups for the same site. The radio user can change the channel selector to select a different Group ID. If the radio has not previously received a Group Restricted message for the newly selected Group, the radio is allowed to attempt to registration on that group. Since the goals and specific implementation of Site Talk Group Restriction vary from one customer to another, guidance should be provided to the radio user on what he/she should do upon learning that a Talk Group is site restricted.

By design, the SU keeps its list of disallowed site/group combinations in non-persistent memory only. The list is automatically built when the radio decodes certain over-the-air messages and supports up to 170 entries for all Connect Plus networks and sites visited by the radio. For example, if Group 100 is restricted at sites 1-10 within Network ID 50 that will equate to 10 different entries on the radio’s blacklist (once the radio has attempted to register one time on sites 1-10). If the list fills, the oldest entry on the list is automatically replaced by the newest entry. If this occurs, the radio will have to make a new registration attempt on the network/site/group combination that dropped off the list in order to learn again that it is a restricted. The list is cleared upon any event that causes an Option Board reset. This includes power cycling the radio, programming the radio or Option Board, etc. After the Option Board clears its internal site blacklist, it will once again attempt to register with any network site while selected to any Talk Group. If the Talk Group record still shows that the site is “disallowed” for the currently selected Talk Group, the process starts over. However, if the SAPR screen information has been updated so that the site is now listed as an “allowed site”, the registration will be allowed, provided that the radio passes all of the normal registration checks.

It is important to understand the following about how the Site Restriction by Talk Group feature works in Connect Plus:

1. <u>Do not configure any Group as disallowed (i.e. restricted) for any site until all radios that use the Group have Option Board firmware that supports the Site Restriction by Talk Group feature</u>. If a radio attempts to register with a disallowed Group, and if the radio does not have Option Board firmware that supports the feature, the controller will send a registration response indicating “Invalid Talk Group ID”. This response effectively disables the radio while selected to that Talk Group. As long as the radio is in this state, it cannot be used at all. The radio user must manually change the channel selector to an allowed Group in order for the radio to initiate a new registration attempt.

2. It is important to understand the interaction between Site Restriction by Talk Group and Emergency. If a radio is searching when the radio user presses the “Emergency On” button, the radio enters “Emergency Pending” state. The radio must first successfully register with a site before it can transmit its Emergency Request. When the radio is searching with Emergency Pending, it will attempt to register with any site of sufficient signal strength that matches the Network ID of the Option Board’s currently selected Connect Plus zone, regardless of whether the radio’s selected Talk Group is restricted for that site. If the Option Board firmware is Release 1.7 (R2.6.0) or later, the radio’s registration request informs the controller that the radio has a pending emergency, which causes the controller to bypass its normal check to determine whether the group is restricted for the site. Following the registration, the radio automatically sends its Emergency call (or Emergency Alert) request, which is processed by the site controller per its normal Emergency handling rules. Once the Emergency Call or Emergency Alert is over, the radio will automatically leave the site and enter search upon decoding an announcement that its currently selected Talk Group ID is site restricted.

3. If the application user configures a group as “restricted” for a site, and if there are radios currently registered to that site on the newly disallowed Group, the controller makes a best effort to inform the current population of the status change. Radios that decode the message will enter search, but this does not guarantee that the radio(s) will find a different site to register on. Until all such radios register at a different network site (or de-register from the network, or re-register on an allowed Group), the controller will continue to show the disallowed Talk Group as registered to the site, and it will continue to transmit inbound network audio and inbound Text Messages that target the disallowed group (subject to resource availability) until all radios are de-registered from that Group at the site.

4. It’s possible that a radio may decode a call assignment message for the disallowed Group prior to decoding the message that informs the radio the Group is not allowed. If this occurs, the radio will join the call for the Group, and the radio user can talk back during Call Hang Time. When the call ends, the radio will have another opportunity to decode the Talk Group restriction announcement.

5. It is possible that the radio user may attempt to initiate a non-Emergency Call on the newly restricted Group before the radio decodes the message that the Group is not allowed on the site. In this event, the controller will not allow the call request. It will respond with a message that informs all site radios selected to the group that the Talk Group is not allowed on the site.

6. It is possible that the radio user may attempt to initiate an Emergency Call or Emergency Alert on the newly restricted Group before the radio decodes the message that the Group is not allowed on the site. In this event, the radio will send its Emergency request, and the controller will honor the request subject to resource availability.

7. If the Connect Plus radio has been informed that a site is disallowed for a specific Group, and then the System Administrator subsequently configures the Group as allowed, the Connect Plus radio will still not attempt to use the site while selected to that Group until the internal blacklist is cleared. The following actions will clear the blacklist; cycling power on the SU, replacing the battery, programming the radio or Option Board, etc.

8. When a radio successfully registers on a site using its currently Selected Talk Group, the controller also registers the radio behind the scenes to the radio’s Multigroup ID and Default Emergency Revert Group ID, depending on how the radio’s unit record is configured in the Connect Plus user database. If the radio’s currently selected Talk Group is allowed, but either the radio’s Multigroup or Default Emergency Revert Group is not allowed, the controller will still register the disallowed Talk Group(s) on behalf of the radio. Upon registering the radios to the disallowed “auxiliary” groups, the controller creates an Event Log entry. Because the controller will transmit inbound network audio and text messages on the disallowed group(s) as long as they remain registered, this is not a recommended configuration. It is recommended to utilize the following guidelines when configuring restricted sites for Group records.

   a. Do not configure a radio’s Default Emergency Revert Group as restricted for any site. Although a radio with supporting firmware can initiate Emergency Call or Emergency Alert on a restricted Group ID, radios with older firmware could be prevented (or delayed) from initiating the Emergency Call or Alert. Additionally, in some scenarios, restricting a Default Emergency Group can limit the number of potential emergency listeners at the same site where a radio initiates the emergency.

   b. Do not configure any Multigroup as site restricted unless of all the regular groups associated with the Multigroup are also restricted for the same site. The Connect Plus infrastructure knows a radio’s Multigroup (if configured properly), but it does not know or track the association between the Multigroup and the regular groups. This association is defined through Option Board programming and can be determined by reading the radio’s Connect Plus codeplug.

9. If the controller sees that a SU is attempting to register on a site with a disallowed Group, it informs the SU of this in response to its registration request. The controller does not perform certain other database

checks for the SU (such as the ESN check). These checks are only performed and enforced when the controller that receives the registration request is an allowed site for SU's currently selected Talk Group.

10. If the radio attempts to register with a site and its Radio ID (SUID) and its currently selected Talk Group ID are both restricted for the site, the SU Site Restriction response takes precedence over the Talk Group Site Restriction. Until the blacklists are cleared, the radio will not attempt registration with that site while selected to any Talk Group.

11. Group Text Messaging is a two-part process: (1) radio sends message to controller, and (2) controller delivers text message to target Group. The radio user can send a Text Message to any Group on its Contact List, even if there is no radio registered to the group at the local site. The controller will accept text messages targeted to a restricted Group, provided that the Group is currently registered to at least one site in the network. The controller will deliver the message at all sites where the target Group is currently registered. Once a group becomes fully de-registered from a site (due to Site Talk Group restriction), text messages to that Group will no longer be delivered to that site.

12. The Priority Monitor checkbox on the Group record is a network-wide setting. So the Priority Monitor checkbox on the Group record can be enabled/disabled regardless of Group site restrictions for the same Talk Group ID. When Priority Monitor is enabled on the Group record, Priority Announcements are made at sites where the Group is registered and active. Once a group becomes fully de-registered from a site (due to Group restriction), there will no longer be any calls or Priority announcements for the group.

13. Site Restriction by Talk Group ID and Permanently Registered Talk Group, which are both site-specific features, are mutually exclusive. A Talk Group cannot be restricted and permanently registered for the same site number.

14. Site All Call ID cannot be configured as a Site Restricted Group.

15. Talk Groups can be restricted via the SAPR screen from registering on XRC Controller sites only. Talk Groups cannot be restricted via the SAPR screen from registering on XRT Gateway sites. However, the same goal can be accomplished via configuration of the XRT User screen in the XRT Configuration Tool software. On the XRT User Screen you can configure a list of Talk Path IDs (i.e. Talk Group IDs) that each XRT Client is allowed to register. Any Talk Path ID not on the list becomes a disallowed ID.

2.12.11 Disable Roam

There are some applications in which the system administrator does not want a subscriber unit to roam between Connect Plus sites. Possible examples are when the Connect Plus system consists of only a single site, or when the SU is being used as stationary dispatch radio. In these instances, the desired behavior is for the SU to remain on the "Preferred Site" that has been configured for the selected Connect Plus zone. When "Disable Roam" is enabled with Connect Plus CPS, the radio will search only the Preferred Site. It is important to remember that even when the "Disable Roam" box is checked, the SU may still enter a state where "Searching" will be shown on the display. This occurs prior to registration with the Preferred Site, or when the SU experiences a loss of Control Channel messaging and the "CSBK Roam Delay" expires, or if Control Chanel RSSI qualifications are not met. However, in this state, the SU will only be searching for its Preferred Site. It will not search any sites that may have been acquired through a Neighbor Site message or the Network Frequency File. Because "Disable Roam" is configurable for each Connect Plus zone, it is possible to restrict searching to the Preferred Site in some zones, while allowing normal roam functionality in others.

2.12.12 Site Lock

In certain situations, the user may have the desire to lock on to a registered site and to prevent the subscriber unit from searching other sites. For example, if the user enters an elevator, the user has knowledge that the radio will have reduced signal strength for a brief period of time. In this scenario, the user may wish to enable Site Lock. Site Lock does not prevent the radio from entering search if the signal from the registered site becomes unacceptable, but it does restrict the radio's search to the site where the radio was registered at the time Site Lock was engaged. This can help the radio return to the registered state (on the desired site) more quickly when the radio re-enters acceptable coverage. Site Lock can be enabled through a configurable short or long button press. When Site Lock is activated, display radios briefly show the message, "Site Locked". When Site Lock is de-activated, display radios briefly show the message "Site Unlocked". Site Lock cannot be activated unless the radio is currently registered to a Connect Plus site. If the user attempts to activate "Site Lock" while in the un-registered state (searching for service), the radio will not activate the feature or display, "Site Locked". When power is recycled, or when the radio user selects a different Connect Plus zone, the SU automatically returns to the "Site Unlocked" state, which allows the radio to search normally. While the Site Lock feature can be helpful in situations such as the one described in this example, a potential drawback is that the radio user may forget to disable "Site Lock", thereby preventing the radio from searching other sites in scenarios where this operation would be desirable.

2.12.13 Connect Plus Performance While Roaming

The Connect Plus radio's ability to automatically search for an acceptable Connect Plus site provides obvious and substantial benefits to the radio user. Even so, it is important to remember that the radio is not registered with any site from the time it initiates Search until it registers with a new site (or re-acquires the previous site). During this time (while the radio is searching), the radio user cannot make or receive calls. For this reason, RSSI thresholds and other Roam settings should be determined with consideration and care. Once the desired settings have been determined, they should not be programmed into large numbers of radios until the desired operation has been confirmed in a smaller set of test radios.

2.12.14 Programmable RSSI Settings

Received Signal Strength Indication (RSSI) is used by the Connect Plus radio to measure Control Channel signal strength. It is determined by measuring the received signal on the Control Channel downlink. RSSI is measured in dBm. Because RSSI is reported using negative numbers, it essentially uses a "reverse" scale where smaller numbers indicate greater signal strength. Connect Plus CPS provides two configurable RSSI Thresholds (RSSI Preferred and RSSI Minimum) and a programmable timer, the RSSI Wait Time. These programmable parameters are utilized by the Connect SU in the following manner:

- The Connect Plus SU will not attempt registration with a site unless the Control Channel RSSI is at the "RSSI Preferred" value, or higher, as configured in the selected Zone Parameters with Connect Plus CPS. When the SU is searching and detects a site that meets "RSSI Preferred", the radio stops its Search and transmits a Registration Request to the site. The Connect Plus SU will not bypass a site that meets "RSSI Preferred" to see if there is a stronger site further down the search list.

- Once registered to a site, the Connect Plus SU continues to measure the Site's RSSI every 3 seconds anytime that the SU is idle and monitoring the Control Channel frequency. If the reported RSSI is ever less than or equal to the "RSSI Minimum" as configured in the selected Zone Parameters with Connect Plus CPS, the Connect Plus SU starts the "RSSI Wait Time" as configured in the selected Zone Parameters with Connect Plus CPS. If the RSSI rises above "RSSI Minimum" prior to expiration of this timer, the radio remains on its registered Control Channel and site. If the "RSSI Wait Time" expires, and

the reported RSSI is still less than or equal to the "RSSI minimum", the Connect Plus radio enters search, even if "CSBK Roam Delay Time" has not expired.

There are several common site configurations that are employed when installing a two-way radio communication system.

1. **Dense Overlapping Coverage (Urban)** – This type of RF coverage consists of sites located close to each, which necessitates utilizing different frequencies for the neighboring sites; refer to Figure 2-8. The non-overlapping sites may reuse the frequencies. A radio user transitions from one site to another within 10-15 minutes.

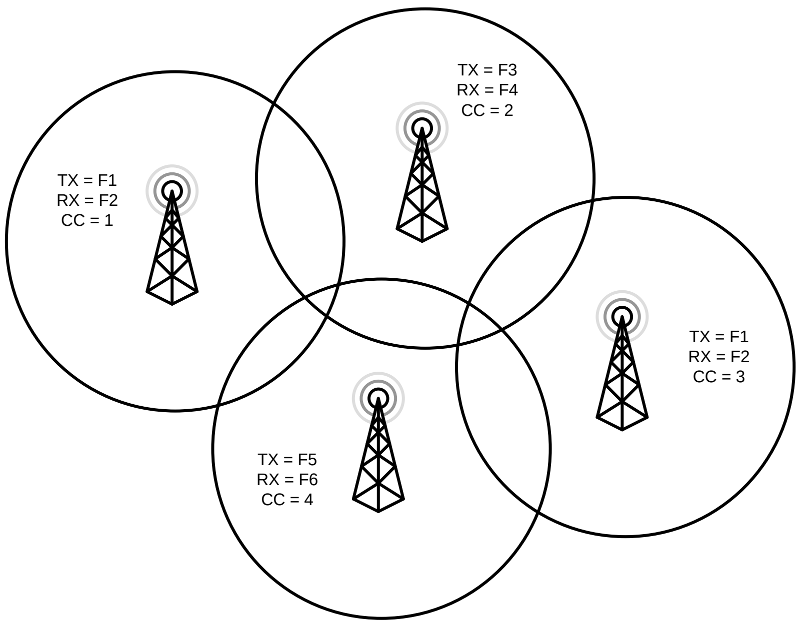


Figure 2-8 **Dense Overlapping Coverage (Urban)**

2. **Isolated Non-Overlapping Coverage (Rural)** – This type of coverage is representative for rural communities, where sites are separate by considerable distance thus proving non-overlapping RF coverage; refer to Figure 2-9. The non-overlapping sites may reuse the frequencies. A subscriber will only be with coverage of one site at a time. A radio user transitions from one site to another within several hours.

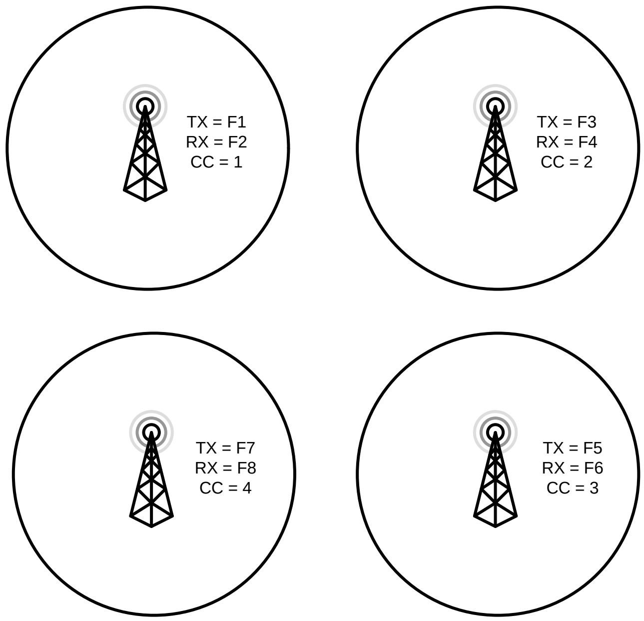


Figure 2-9 Isolated Non-Overlapping Coverage (Rural)

3. **Corridor Coverage** – This type of coverage consists of sites that are placed along various transportation passages, such as roads, train tracks, shore lines, rivers and canals. In such site configuration a pair of adjacent sites overlaps in RF coverage; refer to Figure 2-10. The non-overlapping sites may reuse the frequencies. A radio user transitions from one site to another within an hour.

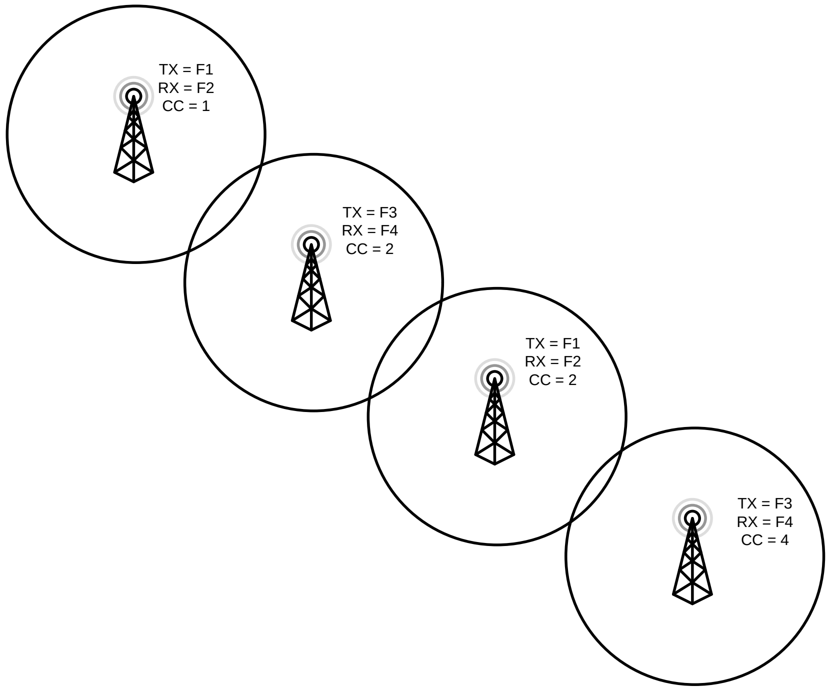


Figure 2-10 Corridor Coverage

4. **Multi-Story Building Coverage** – This type of coverage consists of sites that are situated extremely close to each other with short range coverage and overlap across all sites; refer to Figure 2-11. Such coverage is mostly utilized in multi-story buildings, but can be encountered in other man-made structures, such as tunnels, large vessels or underground passageways. Frequency reuse is not common due to the small coverage footprint usually implemented with in-building radiax antenna systems. Users in such RF coverage also often experience quick signal strength drop offs due to the nature of in building coverage. A radio will only be within coverage of one to two sites at a time. The time it takes a radio user to move from the coverage of one site to another is in the range of one minute.

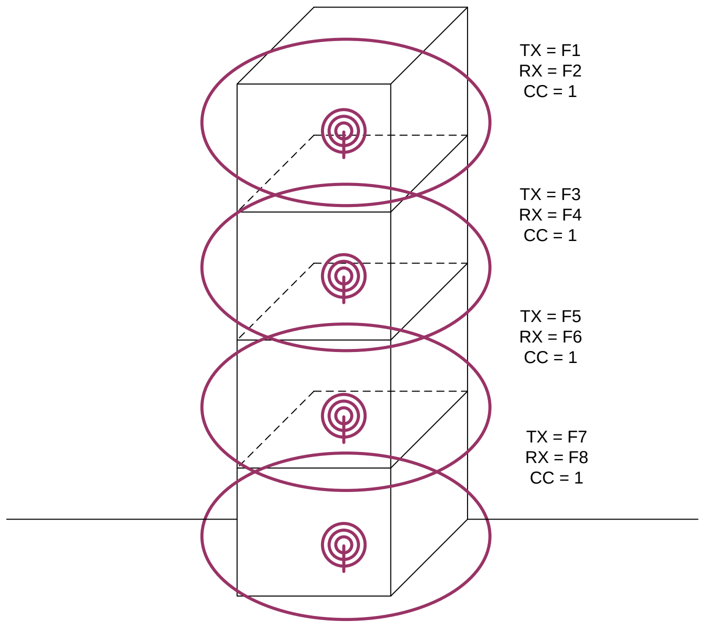


Figure 2-11 Multi-Story Coverage

Depending on the site configuration, the RSSI Preferred and RSSI Minimum values will be set differently; RSSI Wait Time[22] should be set accordingly as well, such that it does not exceed the expected site transition time corresponding to the coverage configuration.

For example, if the customer has a “Isolated Non-Overlapping Coverage” the RSSI Preferred and RSSI Minimum can be set to lowest values allowed by Connect Plus CPS (-120dBm). Since there is no overlap, there is no reason for the radio to start roaming until well outside of the coverage range of the Control Channel repeater. For extremely close sites with large overlap and quick signal drop off like the “Multi-Story Coverage”, it might be better to set to these to higher values, so that the radios will search for stronger sites closer to the repeater. However, note that for such configuration the system designer may take the approach of installing a single site where the Control Channel repeater can be placed in the center of the desired coverage (e.g. middle floor). This of course would be possible when 15 repeaters, or in other words 29 channels, can satisfy the customer communication needs.

[22] Also refer to CSBK Roam Delay Time.

The following table provides the suggested settings for each basic site configuration. Many radio systems will have a combination of site configurations so the system designer will need to take all configurations into consideration and choose an appropriate value.

Site Configuration	Recommended RSSI Preferred	Recommended RSSI Minimum	Recommended RSSI Wait Time	% of Outer Range Radio will Scan
Isolated Non-Overlapping Coverage (Rural)	-120 dBm	-120 dBm	120 seconds	Out of Range
Corridor Coverage	-110 dBm	-115 dBm	90 seconds	10 %
Dense Overlapping Coverage (Urban)	-108 dBm	-113 dBm	30 seconds	20 %
Multi-Story Coverage	-102 dBm	-107 dBm	10 seconds	50 %

Table 2-7 Recommended RSSI Settings

Note that the listed RSSI settings assume the outbound and inbound RF coverage of the system is balanced. In other words, when a radio is within good outbound coverage of the repeater the radio’s inbound transmission can reach the repeater. Since the roaming algorithm uses the outbound transmission to determine when to roam, having an unbalanced system can cause radios not to roam even though they can no longer reach the repeater. This can lead to radio transmissions that do not reach the repeater and are therefore not repeated.

One method to rectify this problem is to lower the output power of the repeater. This decreases the outbound coverage area, but ensures that if a subscriber can hear the repeater well, it can respond successfully. If lowering the output power is not desirable, the RSSI threshold values need to be raised higher (less negative) than the recommended values. This forces the radios to roam to another site within very good RF coverage of another. This value may be different for portables and mobiles since they have different output power and therefore different inbound coverage. Portables may need a higher (less negative) RSSI threshold than mobiles.

Also note that there is one set of RSSI values per Connect Plus zone. This means that if one zone has an inbound outbound imbalance and another does not, it may be difficult to find the optimal RSSI settings to accommodate both zones.

2.12.15 CSBK Roam Delay Time

The Connect Plus radio has another configurable timer that affects when the radio starts to Search. It is called the “CSBK Roam Delay Time”, and is programmable per Connect Plus Zone with Connect Plus CPS. This programmable setting determines how long the radio will continue to listen to the current Control Channel when it doesn’t decode any valid Control Channel messages. If the timer expires, and the radio hasn’t decoded a valid message, the radio starts to search, even if “RSSI Wait Time” has not expired.

2.13 Group Scan in Connect Plus System

MOTOTRBO Connect Plus supports a Group Scan feature. The Group Scan feature allows the subscriber unit to monitor and join calls for Groups other than its Registered Group(s). With conventional radio (non-trunked), the term “scan” usually refers to the ability to scan through a list of channels (i.e. frequencies) and then park on a channel when activity is found. This is NOT what the Connect Plus trunking subscriber unit does while scanning. Connect Plus scan is more akin to the feature known as “Group Scan” in other MOTOTRBO digital modes. In Connect Plus, the SU monitors a single frequency and slot (the Control Channel), as it listens for a number of different Group IDs. Once it detects a channel assignment message for a Group of interest, the Connect Plus

subscriber unit moves to the frequency and slot indicated in the message. This process is described in greater detail in subsequent sections.

There are two types of Group Scan in Connect Plus:

- Automatic Group Scan
- Selectable Group Scan

Note: The Connect Plus radio can also scan for activity on "Priority" Scan Groups while listening to a voice call on its assigned traffic channel. For more information, see the sub-section titled "Connect Plus Priority Monitor Scan".

2.13.1 Automatic Group Scan

Automatic Group Scan is the *default operating mode* of the Connect Plus SU. This means that this is how the Connect Plus SU normally functions and requires no user intervention to activate. In addition, this mode cannot be disabled by the user.

All Connect Plus subscriber units continuously monitor the control channel timeslot when not actively engaged in a call (receiving or transmitting on a trunk-to timeslot). While scanning, the subscriber unit listens for and responds to call assignment messages for the following IDs:

1. Its Unit ID (private calls, text messages, etc)
2. Its Registered Group ID
3. The Site All Call ID. This includes a Network Wide All Call (NWAC), which is initiated by a non-radio device (such as a digital wireline console) and utilizes the Site All Call ID.
4. Its Multigroup ID (if configured)
5. Emergency Calls on its Default Emergency Revert Group ID (if configured)

This type of scanning is automatic, continuously active, and is called "Automatic Scan".
If the Connect Plus SU detects an active call (either in-progress, or during call setup) for one of these IDs, it will join the call. This is the normal, default mode for the Connect Plus SU. This feature cannot be turned off.

In addition to Automatic Group Scan, the subscriber unit may be programmed for *Selectable Group Scan*. This scanning functionality is what most users would normally associate with the term "Group Scan". The remainder of this section will detail Selectable Group Scan.

2.13.2 Selectable Group Scan

Selectable Group Scan can be configured for each subscriber unit in MOTOTRBO Connect Plus Option Board CPS and is an optional configuration item. This type of scanning allows the Connect Plus SU to monitor additional Groups to those normally monitored using automatic scan (see above for details on automatic scan). Each Connect Plus zone may have a scan list configured.

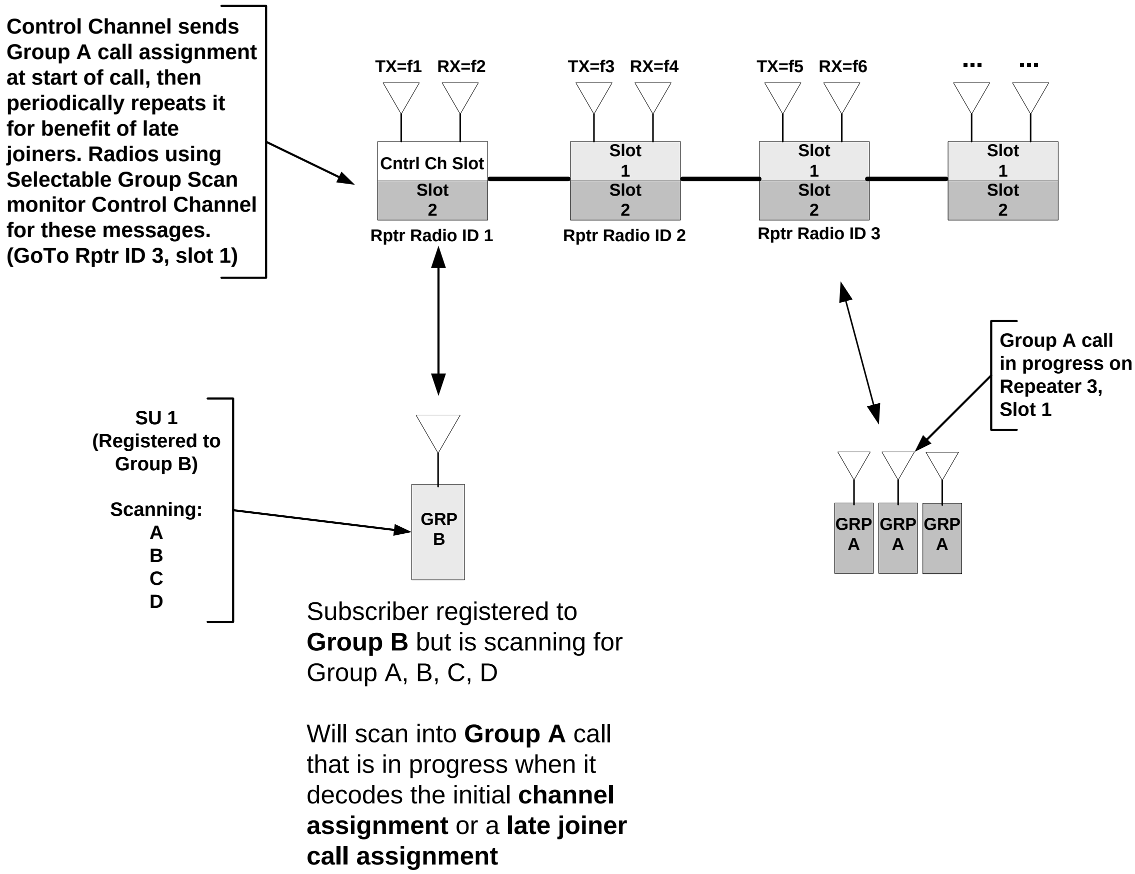


Figure 2-12 Connect Plus Selectable Group Scan

When Selectable Group Scan is enabled for a subscriber unit, the SU is programmed with a scan list. This scan list determines which Groups that the Connect Plus SU will be able to scan into.

When scanning, the radio will scan into calls on a first-come, first-served basis. Upon decoding a call assignment message for any of the IDs in its scan list, the Connect Plus SU will move to the trunk-to timeslot provided in the message. Scanning is “first come, first-served” in that the Connect Plus SU responds to the first of these messages for any ID in its scan list.

Figure 2-12 above shows a Connect Plus SU that is registered to Group B and is monitoring the control channel timeslot. If this subscriber unit decodes a call assignment message for any of its configured scan groups it will switch to the repeater and trunk-to timeslot in the assignment and monitor the call.

2.13.3 Priority Monitor Scan

Connect Plus supports Priority Monitor Scan, an enhancement to the Group Scan feature.

Priority Monitor allows the Connect Plus system to make Priority announcements, on traffic channels, during Group Calls in progress. The Priority announcements allow a Connect Plus radio to become aware of other (priority) calls that are taking place on the site, even while the radio is un-muted to audio on the traffic channel.

When the Connect Plus radio decodes a Priority announcement, it decides whether to stay with its current call, or whether to move to the announced call, based on Connect Plus CPS configuration and logic that resides within the Connect Plus Option Board. If the radio decides to change to a different call, it moves directly to the repeater and slot indicated in the announcement message. It does not go back to the Control Channel prior to changing calls.

Configuring Priority Monitor Scan

A fundamental principle of Connect Plus Priority Scan is that some groups have higher priority than other groups. System configuration determines Group priority. The Group IDs that are configured as Priority groups in the Connect Plus radios must be the same as the Group IDs that are flagged as Priority Monitor groups in the Connect Plus controller. The subscriber radios and the infrastructure must have matching configuration for the feature to work as designed. Therefore, the party responsible for programming the Connect Plus radios and the party responsible for programming the Connect Plus controllers must coordinate closely.

This section discusses how to configure Priority groups in the subscriber radio and in the XRC Controller, and it provides guidelines for selecting and enabling priority groups.

Programming Priority Groups with Connect Plus CPS and/or the radio menu

It is possible to designate one Group per Zone Scan List as a “Priority One” Group and another Group as a “Priority Two” Group. This is accomplished via CP CPS programming, or by using the menu on a display-equipped radio. Any Scan List Group that is not designated as “Priority One” or “Priority Two” is a non-Priority Group.

If desired, “Permanent” Scan Members can be configured as Priority One or Priority Two scan list members. The Permanent Scan members are: (1) the “Current” (Currently Selected) Group, (2) the radio’s “Multigroup”, and (3) the “All Call” (Site All Call) Group.

The radio’s Default Emergency Revert Group ID, which isn’t shown on the zone scan list, is a special case. If the radio’s Emergency Mode for the currently selected Connect Plus zone is Emergency Call, and if the radio is configured to initiate Emergency Call on its Default Emergency Revert Group ID, then the radio automatically makes the Default Emergency Revert Group ID its highest priority scan member. In this case the Default Emergency Revert Group ID has Higher Priority than the Priority One or Priority Two Scan List Member. This is the automatic operation of the Connect Plus radio when scan is enabled (and when “Ignore EM Revert Call RX” is not enabled).

Note: Priority Monitor announcements are not sent for Emergency Alerts. Priority Monitor Scan is for voice calls only.

2.13.3.1 Configuring Priority Groups in XRC Controller with Network Manager

To enable Priority Monitor Scan in the XRC Controller, the Network Manager user must:

1. Enable the Priority Monitor Scan feature in each network site (where the feature is desired) by checking the “Enable Priority Monitor” box under Site Configuration, Non-Critical settings. This checkbox allows

the Priority Monitor Scan feature to be toggled on and off in the controller by checking (or un-checking) the box.

   a. When the box is checked, Priority Monitor scan is enabled for any Group ID that has the “Enable Priority Monitor” checkbox enabled (checked) on its Group record.

   b. When the box is unchecked, Priority Monitor scan is disabled at this site for all Group IDs, regardless of whether the “Enable Priority Monitor” checkbox is enabled (checked), or disabled (unchecked) on the Group record .

2. Check the “Enable Priority Monitor” box on each Group record that should be announced as a Priority Group. This action only needs to occur at one site. When the Network Manager user saves the updated Group record, the controller to which the Network Manager is connected will automatically share the updated record with other Connect Plus sites in the same network.

   Priority Monitor should be checked (enabled) for the following groups:

   a. Any Group that is designated as “Priority One” or “Priority Two” Scan List Group in any Connect Plus radio that utilizes this site or network.

   b. The Network Manager displays a Group record for the Site All Call Group. The Site All Call Group record cannot be edited. Priority Monitor is always enabled for this record.

   c. If any network radio is configured to initiate and receive Emergency voice calls on its Default Emergency Group ID, and if the System Administrator desires the controller to make priority announcements for this Group, the Default Emergency Revert Group’s record in the Connect Plus user database should be enabled for Priority Monitor Scan when configuring the controller with the Network Manager.

While the controller needs to know which Groups have been configured as priority groups in the radios, the controller does not need to know whether the Group flagged is “Priority One” or “Priority Two” in the radio. This is because the controller handles all Priority Groups in the same way, regardless of their priority designation in the radio.

It is highly recommended to flag only the necessary groups as Priority Monitor groups in the controller database. Do not enable the box for Group IDs that won’t be designated as Priority One or Priority Two (or Default Emergency Revert Group ID) in any Connect Plus radio. There is no benefit to sending a priority announcement when there isn’t any radio configured to respond to the announcement.

If the radio user has permission to edit the radio’s scan list via the radio menu, this makes the scan list (including the priority designations) dynamic rather than static, depending on the desires of the radio user. Use the following guidelines when the radio user has the ability to edit the scan list from the radio menu:

- If the radio user has been trained about which Groups should and should not be designated as Priority Groups, then only check the box in the controller database for the Group IDs that have been approved as Priority groups. This is the recommended approach.

- If the radio user has NOT been trained about which Groups should and should not be designated as Priority Groups, then check the box in the controller database for ALL Group IDs that appear on any zone scan list in the radio. This is because the radio user can potentially enable any group on the list as a Priority Group. This approach is not recommended.

The following list provides additional details about configuring Priority Monitor Scan operation in the Connect Plus controller:

1. If the Network Manager user changes the site-wide configuration setting to enable/disable Priority Monitor, the controller does not apply the new setting to calls in-progress when the setting is changed. It applies to subsequent calls only.

2. When the Network Manager user changes the Group record setting to enable/disable Priority Monitor Scan for the group, the controller does not apply the new setting to calls in-progress on that Talk Group ID when the setting is changed. It applies to subsequent calls for that Talk Group only.

3. When enabling Priority Monitor for a specific Group ID, the Network Manager may present a warning message, advising that the Group ID is in conflict in with another Priority Monitor group. This can occur because of the way Priority Announcements are sent over-the-air. The Talk Group ID for a Priority Call is abbreviated if the Group ID number is larger than 262,142. Larger Group ID numbers can be used, but are not recommended. If a larger number is sent, its abbreviated format can potentially look the same to a Connect Plus radio as another smaller Priority Monitor Group ID number. This is called a “virtual duplicate”, and it can cause a radio to respond to an announcement that is not for its “true” Priority Monitor Group ID. If this occurs, the radio will **not** un-mute to the *unexpected* Group, but it can cause the radio to miss audio for the call it leaves. This is why the Network Manager raises a warning when attempting to add a Priority Group that is a “virtual duplicate” to a Group ID that has already been flagged as a Priority Group in the controller database. **The best way to avoid possible Priority Monitor conflicts is to limit all Priority Group ID numbers to 262,142 (or less) wherever possible**.

4. There is a field labeled “Priority” on the Network Manager Group record which supports the configuration of Priority Levels 2 through 8. This setting is not related to Priority Monitor Scan. It is used to help determine a call’s priority for exiting the Busy Queue. For more information, please see the sections called, “Busy Queue” and “Configuring Priority Levels in Connect Plus”.

Selecting Priority Group IDs

One of the most important decisions in utilizing the Priority Monitor feature is which Group IDs to select as Priority One or Priority Two Group IDs. While this decision is determined largely by organizational priorities, the following Group’s merit discussion:

- **Currently Selected Group**: If the Currently Selected Group should have higher priority than Groups in the scan list, then configure the scan list entry called “Selected” in Connect Plus CPS (or “Current” via the radio menu) for the desired Priority (One or Two). This causes the Priority assignment to change dynamically as the radio user changes the channel selector. It follows the currently selected Group Contact. This reduces the chances that the radio user will miss an entire call on the selected group because the radio scanned to a different group while the selected group was idle. If “Selected” is configured as a Priority Group in the radio, then check the “Enable Priority Monitor” checkbox in the XRC Controller for every Group ID that is assigned to a channel selector position in the radio.

- **Multigroup ID**: Many companies or organizations utilize the Multigroup feature for announcements that should be heard by multiple radio groups. Priority Monitor can be utilized to move radios from ongoing group calls to the Multigroup announcement. If the organization’s Multigroup ID is desired as a Priority Group, then configure the Multigroup priority (One or Two) on the radio’s zone scan list, and check the “Enable Priority Monitor” checkbox on the group record for the Multigroup ID in the XRC Controller.

- **Default Emergency Revert Group ID** (Emergency Voice Calls): For radios that should be aware of Emergency Voice Calls utilizing the radio’s configured Default Emergency Group ID, Priority Monitor can move radios from ongoing group calls to the Default Emergency Revert Group voice call. After configuring the Zone Emergency settings for Emergency Voice Call, using the Default Emergency Revert Group ID, there is no additional radio scan list configuration required. In the XRC Controller, check the “Enable Priority Monitor” checkbox on the group record for the Group ID that is used as the Emergency Revert Group. If the Default Emergency Revert Group is flagged as a Priority Group in the controller

database, and if the radio should only respond to Emergency Calls on this ID, then the Default Emergency Group ID should only be used for emergency communications. To prevent the Default Emergency Group ID from being used for non-Emergency voice calls, do not assign it to a channel selector position for any fleet radio.

- **Site All Call ID**: Not every site or network utilizes Site All Call. If this feature is used for system radios, then Priority Monitor feature can be utilized to move radios from ongoing group calls to the Site All Call ID. If Site All Call is desired as a Priority Group, then configure the Site All Call Group priority (One or Two) on the radio's zone scan list. In the XRC controller, Priority Monitor is permanently enabled for the Site All Call group record.

For radios that will be starting calls on Priority Groups, it is helpful to remember that it may take a few seconds to collect radios from other ongoing calls. For example, if using the Multigroup for an organization-wide announcement, the speaker may wish to say something like, "Please stand by for an announcement in 5, 4, 3, 2, 1" prior to making the announcement. This provides time for radios on other groups to change calls, and it increases the chances that all radios will hear the critical announcement content. The amount of time needed to collect radios from other calls depends on the factors discussed in the sub-section called, "Sending and Responding to Priority Call announcements."

2.13.3.2 How Priority Monitor Scan Works

Whenever a Group Call becomes active on a Connect Plus site, the controller checks to determine (1) if this Group ID is designated as a Priority Monitor Group in the controller's database and (2) whether there are any regular Group calls (on different Group IDs) currently in progress on the site. To illustrate how this works, let's use an example where there is a call already in-progress ("Call A") when a different call starts on a priority group ("Call B").

The controller not only assigns a timeslot for "Call B", it also begins a Priority Announcement for "Call B" on the downlink for the in-progress, "Call A". The announcement does not interrupt the audio for radios that are un-muted to "Call A. The "Call B" Priority Announcement will be periodically sent on "Call A" until either "Call A" or "Call B" ends (whichever occurs first).

In this same example, it is possible that the "Call A" Group ID is on the controller's Priority Monitor list also. In that event, the controller will not only announce "Call B" on the "Call A" traffic slot, it will also announce "Call A" on the "Call B" traffic slot.

Here are some additional, important, details about how the feature works:

- Merely listening for a higher priority call announcement does not create any audio holes in the radio's current call. However, if the Connect Plus radio leaves its current call to join a higher Priority call-in-progress, this will cause a small audio hole.

- The radio makes its decision to stay with the current call (or to change to a new call) based on the following rules:

    - The radio will not leave an Emergency Call, a Multigroup Call, a Site All Call, a Private voice call (including Remote Monitor and Private Phone Call), or a data call due to Priority Monitor Scan.

    - The radio will leave a regular Group Call to join a higher Priority Group Call, provided that all of the following are true:

        - Scan is currently enabled.

- The Connect Plus radio decodes a Priority Group announcement for a Group that is a higher Priority than the current Group Call in-progress.

- The Priority Monitor Scan feature can cause a radio to make multiple call changes. The example below is not expected to be common, but is possible:

  First change: Radio leaves non-priority Group call for Priority Two Group Call.

  Second change: Radio leaves Priority Two Group Call for Priority One Group Call.

  Third change: Priority leaves Priority One Group Call for Emergency Voice Call on its Default Emergency Revert Group ID.

- When the radio leaves a call in-progress for a higher Priority Call, the radio user should not expect to hear any more of the former (previous) call. The radio user will only hear more of the previous call if (a) it is still in-progress when the Priority Call ends and (b) it is first call assignment of interest that the radio decodes after returning to the Control Channel slot.

- In certain “race” conditions, the radio may leave an ongoing call to join a higher priority call, but the higher priority call may end before the radio can complete the call change. In such a scenario, the radio does not return the previous call, but returns to monitoring the Control Channel. After returning to the Control Channel timeslot, the radio responds to the first decoded call assignment message of interest.

- When the radio leaves a call in-progress for a higher Priority Call, the radio user will join the new call as “late entry”. The user will not hear any of the conversation that took place before his/her radio completed the call change.

- When the radio scans into a Priority Call, it plays a special alert tone, followed by Call Receive Tone (if enabled on the Contact record of the group being received). The radio then un-mutes to the Priority Group.

- Because Priority Monitor Scan is part of the Connect Plus scan feature, the following scan rules also apply to Priority Monitor:
  - The Connect Plus radio only responds to Priority Monitor announcements when scan is currently enabled in the radio. The controller doesn’t know when scan is toggled on or off in the radio, so it always attempts to send Priority announcements for Groups that are designated as Priority Monitor groups in its database.
  - Scan Talkback enable/disable (a configurable option in Connect Plus CPS) works the same way for any scanned call, regardless of whether the scanned Group is a Priority One or Priority Two Group. For more information, see the section called, “Participating in Selectable Scan Calls”.

2.13.3.3 Sending and Responding to Priority Call Announcements

A radio cannot change calls to join a higher priority call until it has decoded the announcement for the higher priority call. Therefore, it is important to understand the following details about when (and how quickly) Priority Announcements are sent by the controller/repeater, and when they will be decoded by the radio.

1. Just because a Group is designated as a Priority Group on the radio’s currently selected zone scan list, this does not mean the controller will always broadcast transmissions for this group when they originate at other network sites. Priority Group IDs are just like any other scanned Group ID in regards to the following: The Group may be active elsewhere in the network, but the scanning radio won’t hear the conversation unless (a) there is at least one radio registered to the Group at the local site (or Permanent

Talk Group Registration has been enabled for the Group), and (b) there is an available traffic channel resource at the local site.

2. Only one Priority Group Call can be announced per Priority announcement message. Therefore, if multiple Priority Groups are active on the site, then multiple Priority Announcements are sent during ongoing Group Calls. The Priority Groups are announced one-at-a-time. Consequently, if a large number of Priority Groups are active, it takes longer to announce all Priority Calls, and the "late entry" time is longer.

3. The amount of time that it takes to send Priority Announcements depends on whether the repeater (where the Priority Announcement is sent) has the active Control Channel on timeslot one, or whether both repeater timeslots are currently being used as traffic slots.

    a. If the repeater has the active Control Chanel on timeslot one, it transmits Priority Announcements at a rate of approximately two Priority Group announcements per second. These announcements benefit the radios that are listening to a Group Call on timeslot two. Therefore, if announcements must be sent for eight different Priority Group calls, this will take at least four seconds.

    b. If neither repeater timeslot is currently used as Control Channel, the Priority Announcements are sent at a rate of approximately four Priority Group announcements per second. Therefore, if announcements must be sent for eight different Priority Group calls, this will take at least two seconds.

4. A subscriber radio must be receiving a group call to decode a Priority Announcement. The radio cannot decode Priority Announcements while transmitting. Therefore, if a radio misses a Priority Announcement because it is transmitting, it must wait for the announcement to be sent again while it is in receive mode. How quickly the announcement can be sent again by the controller and repeater is influenced by the factors previously discussed.

5. In certain scenarios a Priority Announcement may never be sent during some calls. Should this occur, the controller will create an Event Log entry, "Priority Announcement Not Sent". The Event log entry will capture the Priority Group ID that was not announced, the Group Call ID that was ongoing at the time (and that didn't carry the announcement), and the repeater where this occurred. The message will also include a reason why the Priority Announcement was not sent:

    a. Priority Call ended prior to announcement.

    b. Repeater went idle prior to announcement.

2.13.3.4 Interaction of Priority Monitor Scan and Roaming

The Priority Monitor feature has a slight impact on radios that are "Searching" for service. If the site repeaters are sending Priority Monitor announcements, it may take the radio up to 120ms longer to locate and verify the site's active Control Channel (which the radio must do before it sends its registration request). The cumulative impact to Search times is more pronounced when (a) each site has multiple Control Channels to search and (b) when the Option Board must search through many sites prior to locating an acceptable site and signal.

If the Connect Plus controller(s) will be sending Priority Announcements, it is recommended to upgrade Connect Plus Option Board firmware to a level that understands Priority Monitor messaging, even if the radio will not be configured to use Priority Monitor. This will help the radio's Searching performance, especially when each site has multiple Control Channels in the Option Board's Network Frequency File.

If the radio network utilizes Priority Monitor messaging, it is recommended to examine the Option Board's Roam Dwell Time setting (configurable with Connect Plus CPS). If Roam Dwell Time is configured for 240ms (the

minimum configurable value), this is right on the edge for acceptable roaming performance when Priority Monitor signaling is utilized. If radios seem to be by-passing otherwise acceptable sites while searching, then the Roam Dwell Time value should be increased by at least 120ms.

2.13.4 Participating in Selectable Scan Calls

If the radio scans into a call from the selectable group scan list, and if the radio user presses PTT during the scanned call, the radio's operation depends on whether Scan Talkback was enabled or disabled during radio programming.

Scan Talkback Disabled: The radio leaves the scanned call and attempts to transmit on the contact for the currently selected channel position. After the call on the currently selected contact, the radio waits until its Scan Hang Timer expires before it joins another call from the selectable group scan list.

Scan Talkback Enabled: While scanned into a call that is not its registered Group, the Connect Plus SU can participate as would any other user by pressing the PTT during the call hang time period. When transmitting, the SU will use the same ID as the scanned call. However, if the radio user presses PTT after the call hang time expires, the SU will request to start a new voice call on its currently selected Contact Name. This may be a different ID than the scanned ID of the previous call.

2.13.5 Radio Indications during Selectable Group Scan

When Selectable Group Scan is turned-on, the Connect Plus SU has the following indications:

- When scan is turned on via the programmable button or menu option, the display will show "Scan On" momentarily (display radios only).
- The radio provides a tone that ascends in pitch
- The display shows the scan icon (display radios only).
- While the radio is monitoring the control channel timeslot with Selectable Group Scan active, the top LED blinks orange. While listening to a call on a trunk-to timeslot, the LED operates as it normally does for the call type.

2.13.6 Radio Indications when turning off Selectable Group Scan

When Selectable Group Scan is turned-off, the Connect Plus SU has the following indications:

- When scan is turned off via the programmable button or menu option, the display will show "Scan Off" momentarily (display radios only).
- The radio provides a tone that descends in pitch
- The display no longer shows the scan icon
- While the radio is monitoring the control channel timeslot with Selectable Group Scan turned off, the top LED blinks green.

2.13.7 Rules Governing Selectable Group Scan

There are a number of rules that govern Selectable Group Scan. If these are not well understood, then some system behavior might be interpreted as malfunctions or nuisances.

2.13.7.1 "Preferred Site" and Group Scan

Selectable Group Scan is available while the radio is registered to any network site.

Since "Preferred Site" is a zone parameter in Connect Plus, different Connect Plus zones can be configured with a different "Preferred Site". This is especially useful for a subscriber unit that will be utilizing multiple single-site systems. Each of these systems can be programmed into a different Connect Plus zone. In this configuration each single site can be treated as a "Preferred Site" with Selectable Group Scan available.

2.13.7.2 User Notification at Non-Preferred Sites

In Connect Plus multisite, the subscriber unit is not typically programmed with a different Connect Plus zone for each site. The most common configuration is for the Connect Plus SU to automatically roam to multiple sites while selected to a single Connect Plus zone. In this configuration, the subscriber unit will be visiting sites that are not its "Preferred Site" for the currently selected zone.

2.13.7.3 Assigning Groups to a Knob Position

Connect Plus supports a configurable scan list per Option Board zone, up to a maximum of sixteen Connect Plus zones. Each Zone Scan list can contain up to 16 configurable Group members. Connect Plus CPS is used to build the zone scan list (i.e. add and delete groups). In some radio models, the radio user can also add groups to the zone scan list and delete groups from the zone scan list via the menu. This requires a display-equipped radio that is enabled for the Connect Plus CPS Scan menu "Edit List" option. For more information on this feature, see the Connect Plus subscriber radio user guide for the specific model of interest.

Connect Plus enforces the requirement that a contact must be assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) in order for it to be placed on the scan list. If a contact is not assigned to a channel selector knob position, it is not available to be added to a zone scan list. This requirement ensures that the radio user will be able to select and start a call on the scanned Group if he/she cannot respond to a call prior to expiration of the call hang time.

Connect Plus CPS populates the "available members" of the Zone Scan list with Group Contacts that have been assigned a Channel Selector Knob/Channel Rocker position in any Connect Plus zone. While this enhancement allows the radio user to scan Groups assigned to a Channel Selector Knob/Channel Rocker position outside of the current zone, the radio user should be aware of the following:

1. Even though the scanned Group resides in another zone, the Zone Parameters of the currently selected zone still take precedence. The Transmission Settings, OTA File Transfer Settings, Roam & Search Settings, and Emergency Settings of the selected zone are still in effect.

2. If the radio scans into a Group call on a contact that is not assigned to a Channel Selector Knob/Channel Rocker position in the selected zone, and if the radio user wishes to speak on this Group Contact after the Call Hang Time expires, he/she will have to change to a Connect Plus zone where this Group is assigned to a Channel Selector Knob/Channel Rocker position in order to start a call to this Group.

3. If the radio scans into call on a Group Contact from another zone, the alias displayed by the radio is governed by the following rules:

   a. If the scanned Group ID also has a contact record in the currently selected zone, the Connect Plus radio will display the alias from the contact record of the selected zone.
   b. If the scanned Group ID does not have contact record in the currently selected zone, the alias will display as configured on the contact record in the zone that supplied the contact information.

2.13.8 Missed Calls

The Connect Plus SU misses calls for IDs in its selectable scan list under the following conditions:

- User has disabled the scan feature via the programmable button or menu option.
- Subscriber Unit is not monitoring the control channel timeslot (already engaged in a call on a trunk-to timeslot). In this case, the radio will only be informed of calls for “Priority” scan groups. For more information, see the section titled “Priority Monitor Scan”.
- No member of the target Group is registered at the site.

2.13.9 Multisite Considerations with Group Scan

When implemented in a single-site system, Selectable Group Scan is highly reliable and robust. However, when implemented in a multisite system, there are situations that cause the subscriber unit to miss calls in their scan list. The primary reason for this is that, unless the Group has been placed on the site’s list of permanently registered Groups, *audio is not provided to sites that do not have a Group member registered at the site*.

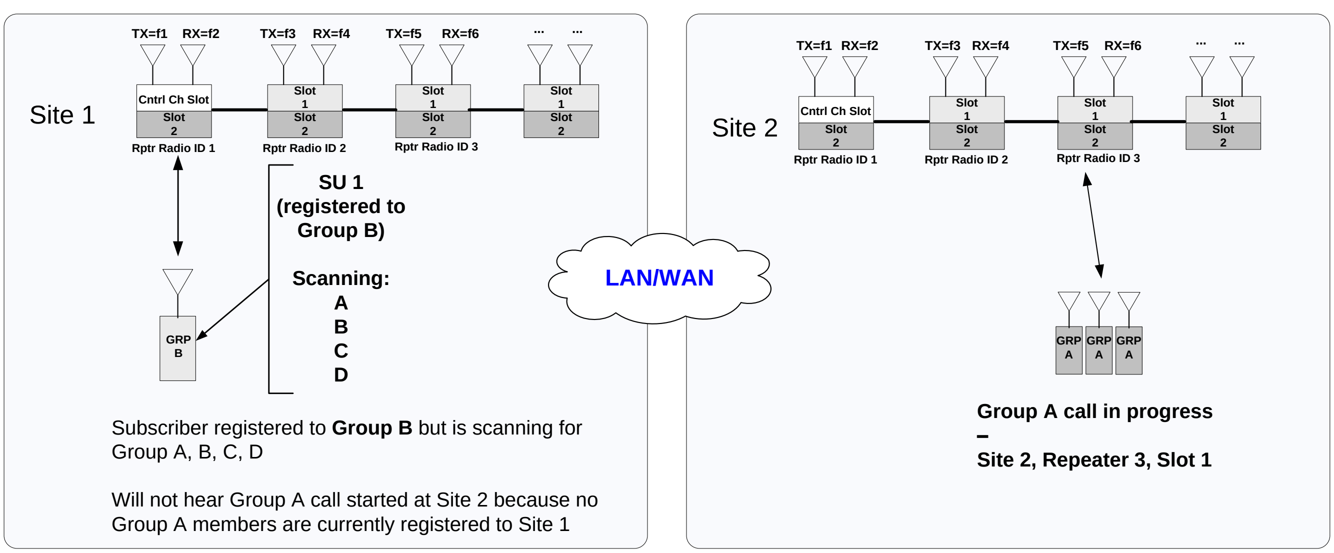


Figure 2-13 Audio Not Available at Site without Registered Group Member

2.13.9.1 Transmitting Audio Inbound from the Network

In the Connect Plus default system configuration, a site does not provide Group audio or call assignment messages unless there is a Group member currently registered to the site. This important feature, known as "dynamic site assignment", helps conserve RF resources as well as IP bandwidth between sites. However, it also has implications for the Selectable Group Scan feature in a multisite environment. In the figure above, a SU is registered to Group B at Site 1 (its Preferred Site), and is also scanning Groups A, C and D. Because there is no unit currently registered to Group A at Site 1, the Connect Plus network has no reason to route calls to that site. Therefore, when a call starts on Group A on Site 2, the SU registered to Group B at Site 1 will not be aware of the call.

The Permanent Talk Group Registration feature can be utilized to enhance network scan operation by configuring a list of Groups that should remain permanently registered to a Connect Plus site. When a Group is permanently registered, and when the Group is active elsewhere in the network, the local site controller will transmit audio for the group (subject to repeater resource availability), even when there isn't any radio currently selected to (and registered to) the group at the site. This increases the chances that a scanning radio can hear transmissions for all of its scan list groups. For more information, see section "*Configuring Permanently Registered Groups*".

2.13.9.2 System Less Aware of Target SU's Current Availability

When a subscriber unit is participating in a call on its registered Group, the controller is aware that the SU is unavailable, and it will not attempt to contact the SU with an individual call (Private Call, text message, etc.) until the call on the registered Group is over. However, when the SU has scanned into a call on a Group to which it is not currently registered, the site controller is not aware that the radio is not available to receive other calls. For calls targeted to this Connect Plus SU, it is likely that the controller will try to contact the SU, and may attempt several re-tries before determining that the SU is not currently available. In the meantime, the radio that is initiating the call to the unavailable SU will be tied up in the call attempt until the controller determines that the target SU is unavailable. If the call being sent to the SU is a Controller Initiated Radio Check (CIRC), and if the SU doesn't respond because it has scanned into a call for a Group ID to which it isn't registered, this can result in the SU being prematurely de-registered from the site.

2.13.10 Differences in Scan from Other MOTOTRBO Digital Modes

The primary differences between scan in Connect Plus and other MOTOTRBO digital modes are described below:

- **Subscriber Unit Monitors Control Channel and Assigned Voice Channel Only**
  In Connect Plus, the subscriber unit only monitors the control channel (while idle) and its assigned voice channel slot timeslot (while receiving a regular voice call) for information about calls involving members of its scan list. It does not scan for calls by hopping to different frequencies.

- **Connect Plus scans only the Group Scan list for the selected Connect Plus zone**
  The Channel Scan feature provided by some non-Connect Plus modes allows the radio to scan between channels in different zones and even between channels operating in different modes (analog and digital, for example). Connect Plus does not support scanning between different zones and/or modes. However, it does allow Groups from other zones to be placed on the zone scan list, provided that the two zones share the same Network ID.

- **Interactions between Scanning & Roaming**
  In non-Connect Plus digital modes, a single channel can be enabled for a Scan list or a Roam list, but not both. Configuring a scan list for a Connect Plus zone does not affect the SU's ability to automatically roam to other Connect Plus sites.

- **Connect Plus Scan does not Require a "Preamble"**
  In other MOTOTRBO digital modes, a number of preamble messages are typically sent prior to data calls in order to increase the likelihood that a scanning radio will hear the call. The "TX Preamble Duration" is a configurable parameter on the MOTOTRBO CPS General Settings screen. Because a Connect Plus radio does not hop frequencies while scanning, it does not require a Preamble. The "TX Preamble Duration" should be **set to zero (0)**.

2.13.11 Interactions of Scan and Emergency

This section provides a brief discussion of the interactions of the Scan and Emergency Features in Connect Plus.

Scanning the Default Emergency Revert Group ID:

If a Connect Plus radio is configured for a Default Emergency Revert Group ID, and if the radio is <u>not</u> configured to "Ignore EM Revert Call RX" (Ignore Emergency Revert Call Receive), then it always scans for Emergency Calls or Emergency Alerts (depending on Connect Plus CPS programming) on that ID no matter where it goes in the network. However, the Connect Plus radio does not scan for non-Emergency Calls on this ID unless it happens to also be (a) its currently Registered Talk Group ID, (b) its Multigroup ID, or (c) a currently enabled member of the scan list (if the radio is currently registered to its Preferred Site and scan is turned on). Note: When the Default Emergency Revert Group is used with the Emergency Alert feature, it should not be used for any type of voice call within the same network. It should only be used to send an Emergency Alert. For information regarding the interaction of the Default Emergency Revert Group ID and Priority Monitor Scan, see section titled "Priority Monitor Scan".

Responding to Emergency Calls:

The Connect Plus SU will respond to an Emergency Call for any of the following IDs: (a) its Emergency Revert Group ID (if configured with one), (b) its Multigroup ID (if configured with one), (c) its currently Registered Talk Group ID, (d) any currently enabled member of the scan list. A Connect Plus radio only responds to an Emergency Alert when it matches the SU's Default Emergency Revert Group ID.

When the Emergency Call ends:

If the Connect Plus SU scans into an Emergency Call, and then the Emergency Call ends, the SU returns the Control Channel timeslot and scans for IDs of interest as described in previous sections. If the radio user presses PTT to start a call, the MOTOTRBO core series SU will request a non-emergency voice call on the Contact Name that has been programmed for currently selected Channel Selector Knob (portable radio) or Channel Rocker (mobile radio) position. The MOTOTRBO enhanced series SU will not initiate a call unless the currently selected Zone and Group matches the details on the Emergency Alarm Details screen (if displayed). The radio user should dismiss the Emergency Alarm Details screen if he/she wishes to initiate a call on a different Group.

2.13.12 Configuring Permanently Registered Groups

Permanent Talk Group Registration can be used in conjunction with the Connect Plus scan feature to enhance the radio user's scan experience in a multisite network.

In the Connect Plus default system configuration, a site does not provide Group audio or call assignment messages unless there is a Group member currently registered to the site. While this operation provides for highly

efficient resource utilization, it also means that scanning radios are dependent on the registrations of other radios to hear audio for all scanned groups. If no radio is currently selected to a scanned group on the local site then the local site controller does not transmit calls for this Group that are initiated at other network sites. This can cause the radio user to think the Group is inactive, when in reality the Group is active at other sites. To help ensure that audio will be transmitted for all scan groups of interest, regardless of whether any radio is currently selected to the group, the Group can be added to the site's list of Permanently Registered Groups.

The Permanently Registered Talk Groups feature is configured on the Site Access and Permanent Registration (SAPR) screen in the MOTOTRBO Connect Plus Network Manager software application (when connected to an XRC Controller site) or in the MOTOTRBO Connect Plus Configuration Tool application (when connected to a XRT Gateway site). Because the Permanently Registered Talk Groups information is stored behind the scenes as part of the user database, the Permanent Talk Group settings configured via the SAPR screen are automatically shared with all other sites in the same Connect Plus network. It is not necessary to configure the same information at multiple sites. To the contrary, it is recommended to make all SAPR screen edits at only one designated network site. The Permanently Registered Talk Group settings are not visible when viewing a Group record in the User Registration screen. Because the User Registration Screen and the Site Access and Permanent Registration (SAPR) Screen are both capable of modifying information in the Connect Plus user database, it is not recommended to open both screens at the same time.

The Site Access and Permanent Registration screen provides two ways to configure permanently registered sites for Talk Group IDs:

- From the site perspective view, the application user can add or remove one or more Talk Groups from the site's list of permanently registered Talk Groups.
- From the Talk Group perspective view, the application user can add or remove one or more permanently registered sites for a specific Talk Group ID.
- The following configuration rules pertain to Talk Group permanent registration by site:
  - Talk Groups can be permanently registered to XRC Controller sites only. Talk Groups cannot be permanently registered to XRT Gateway sites.
  - The same Talk Group cannot be on both the restricted list and the permanently registered list for the same site. The features are mutually exclusive.
  - Site All Call ID cannot be configured as a permanently registered group. This is unnecessary because radio-initiated site all call transmissions are always carried on the originating site, but are not networked to other sites.
  - Multigroups cannot be configured as permanently registered. This is unnecessary because the controller automatically registers a radio's multigroup on behalf of the radio, even if the radio is not physically selected to its Multigroup ID.
  - The number of permanently registered groups that are configured for any specific site cannot be greater than 100.

For more information on how to configure Permanently Registered Talk Groups, please see the XRC Controller User Guide.

The purpose of Permanent Talk Group Registration is to enhance the radio user's Talk Group scan experience in a multisite network. If the scan feature is not utilized, then no Groups should be permanently registered, as this would only consume additional resources without providing any benefit to radio users. Additionally, the feature is not needed for a single site network since calls can only be initiated locally, and at least one radio has to be registered to a Group in order to initiate a call to the Group.

If using the Permanent Talk Group Registration to enhance the Talk Group scan feature, it is important to understand the following trade-offs:

- Audio and text messages inbound from the network that target a permanently registered group will still be carried on the site repeaters (subject to resource availability), regardless of whether there are any radios at the site that are interested in the transmission.

- Permanent Talk Group Registration can be expected to increase the number of calls that a site transmits when compared to the default system operation (which is to only transmit audio when at least one radio is registered to the Group).

  - "Busy" conditions (requiring a wait in the Busy Queue) will be more frequent than at sites that don't have permanently registered groups.

  - Repeater airtime will be greater than at sites that don't have permanently registered groups.

- IP bandwidth between sites must be sufficient to handle the networked calls triggered by the permanent registration feature. For each permanently registered talkgroup, when audio is routed to the site, 15 kbps (or 23 kbps with VPN) of bandwidth will be consumed at the originating *and* the receiving site, even if there are no subscribers registered on the said talkgroup at the receiving site. For more information on the IP bandwidth calculations, refer to section "Required Bandwidth Calculations (no VPN)".

Determining which Groups are Permanently Registered to a Site

The Network Manager application provides several ways to determine which groups are permanently registered to a site, and how they are impacting repeater resources:

- The Site Access and Permanent Registration screen can be used to generate a list of groups that are configured as permanently registered for the entered site number.

- On the Site Status screen, when viewing the currently registered groups for a specific site, if [P] appears next to a Group Record Type, this indicates the Group is a permanently registered group for the site. The "Units in Group" information shows how many actual radios are currently selected to (and registered to) the Group. If "Units in Group" is 0 (zero), this indicates that no actual radios are currently selected to (and registered to) the Group.

- The XRC Controller creates an Event Log entry when all eligible voice resources are busy and when there is at least one call currently active for a Permanently Registered Group ID that has no radios registered to the group at the local site. This is helpful for evaluating how Permanently Registered Talk Groups are contributing to "All Trunk Busy" (ATB) conditions at the site. However, the Event Log entry does not (and cannot) indicate whether any radio users were listening to the call. The controller does not know which radios are scanning for activity on which Talk Groups.

2.14 Network ID

A Connect Plus radio must be programmed with the Network ID that is transmitted by the site controllers in its Connect Plus Network. A single Connect Plus radio can be configured with up to sixteen Network IDs, as configured on the Connect Plus CPS Networks Screen. For more information on configuring a single Connect Plus radio with Multiple Network IDs, see the sub-section "Configuring a Connect Plus radio to use Multiple Networks". Defining the Network ID is also part of creating a Network Frequency File.

When a Connect Plus SU searches for service, it will not attempt to register with a site until it verifies that the Network ID being transmitted on the Control Channel downlink agrees with the Network ID that was configured

into the radio with Connect Plus CPS. This check prevents the SU from accidentally attempting to register with Connect Plus sites that are under different ownership, but located in the same geographical area and using some of the same frequencies and color codes as Control Channels within its own network.

The Network ID transmitted on the Control Channel downlink is set by the factory, and is based on information received at time of sale. All Connect Plus controllers under the same ownership are given the same Network ID, unless requested otherwise. Connect Plus controllers under different ownership are typically issued different Network ID. If there are unusual circumstances where controllers under different ownership will be part of the same Connect Plus Network, this information should be communicated to the sales representative at time of purchase since the controllers will need to be issued the same Network ID. If it becomes necessary to change a controller's Network ID after the controller has been deployed to the field, this can be accomplished remotely provided that the required connections are in place.

Relationship of Network ID to Site Number

Each site controller that will be connected together for the purposes of Wide Area Networking must have the same Network ID, but a unique Site Number. The Connect Plus Site Number is programmable in the controller by using the MOTOTRBO Connect Plus Network Manager software. Site Numbers are also important when programming the Connect Plus SU with Connect Plus CPS. Each Connect Plus Zone must be programmed with a "Preferred Site" number. The Site ID is also part of Network Frequency File configuration.

Configuring a Connect Plus radio to use Multiple Networks

The Connect Plus radio can be configured with up to sixteen Network IDs (and up to sixteen Network Frequency Files), but it is only able to use these Network IDs one-at-a-time, depending on which Network ID is configured for the currently selected Connect Plus zone. In order to change from using one network to a different network, the radio user must change the selected Connect Plus zone. This will cause the radio to begin searching the Frequency File for the newly selected network. When the radio user selects a zone for a different network, the Connect Plus radio does not automatically de-register from the previous network prior to searching for the new network. The Network Manager Site Status screen will continue to show that the SU is still registered to the previous site and network until the SU Inactivity Timer expires, and the SU is de-registered after failing to respond to a controller-initiated radio check.

From the infrastructure side, different networks operate independently of one another. The XRC Controller routes calls to other sites that share its same Network ID, but it does not route calls to any site with a different Network ID. Even with these constraints, the radio's Multiple Network ID feature is helpful for certain use cases, such as a technician who is responsible for maintaining equipment for multiple Connect Plus networks.

For every network that will be used by the radio, there must be a user record for the SU's Radio ID in the XRC Controller(s) for that network. The user record only needs to be created (or edited) in one XRC Controller per network, and then it will be automatically propagated to other sites in the same network (assuming that there is connectivity between all network sites).

Because the Radio ID (SUID) is a radio-wide parameter that is configured with MOTOTRBO CPS, the radio will use the same Radio ID in every network that is uses. The radio can have a different Multigroup ID and a different Default Emergency Revert Group ID on each different network, but it must use the same Radio ID. This implies that there must be some communication between the administrators of the different radio networks. Otherwise, the Radio ID used by the SU may not be available in all networks.

Consider the following **example**: Radio 1 has previously used only Network 50, where it has a user record containing its Radio ID (1) and Serial Number and/or Physical Serial Number. Now, it is desirable for this same radio to also use Network 60. In addition to the programming that must be accomplished in the radio with Connect Plus CPS, use the MOTOTRBO Connect Plus Network Manager to create in a user record in the Network 60 controller(s) for Radio ID 1 with this same radio serial number (and/or physical serial number). Otherwise, this radio will not be able to successfully register on Network 60. If there is already a Radio 1 (with a different serial

number or physical serial number) configured in the user database for Network 60, then one of the two radios will have to be assigned a different Radio ID. Both radios will not be able to use the same network with the same Radio ID, but different serial numbers or physical serial numbers. Only the Radio ID/serial number (or physical serial number) combination that matches the user record in the controller database will be allowed to register.

When configuring the SU with Connect Plus CPS, there are three major steps to configure a single radio to use multiple networks:

1. **Configure the Connect Plus CPS Networks Screen**. This screen is used to define which Network IDs will be used by the SU, and it is also used to define which Multigroup ID and Default Emergency Revert Group ID the SU will use on the indicated network.

    a. When a new Network ID is added to the Networks list, the Multigroup ID defaults to 1000. However, the user still needs to create a Multigroup Call contact record. To create the Multigroup Call contact record:

        i. Assign the new Network ID to a Connect Plus Zone. This is done by selecting a zone from the tree view (add a new zone, if necessary), and then select the desired Network ID from the drop-down Network ID list on the General Zone Parameters screen.

        ii. In the same Connect Plus Zone, right-click “Contacts” from the tree view, and select *Add→Multigroup Call* from the pop-up menu. This will create a Multigroup Call contact record. For the Call ID, Connect Plus CPS uses the number defined for “Multigroup ID” on the Networks screen.

    b. When a new Network ID is added to the Networks list, the Default Emergency Revert Group ID defaults to “None”. The next step is to assign the new Network ID to at least one Connect Plus zone (see previous item) and to create Group Call contacts for that zone. Then, return to the Networks Screen to select the desired Default Emergency Revert Group Contact from the drop-down list.

2. **Assign a Network ID to each Connect Plus zone using the Connect plus CPS Zone General Settings Screen**. After defining the Network IDs on the Connect Plus CPS Networks screen, use the General Zone Settings screen to assign one of those Network IDs to each Connect Plus Zone that is defined in the Option Board codeplug.

    a. A single zone can only be assigned to one Network ID. This is the only Network ID that the SU will use while operating in this zone. If the SU is searching for service and detects a site with a matching Network ID, it will attempt to register (provided that the site is not on the SU’s internal “blacklist” due to the Site Restriction feature, and provided that other criteria such as RSSI are met). However, if the SU detects a site with a Network ID other than the one defined for this zone, it will not attempt to register – even if the Network ID is permitted for a different zone in the same radio.

    b. It is allowable to assign more than one Connect Plus zone to the same Network ID. All zones that are assigned to the same Network ID share the same Multigroup ID, the same Default Emergency Revert Group ID, and the same Network Frequency File.

    c. When a new zone is added, it defaults to Network ID zero (as a placeholder until the zone is assigned to a network). Network ID zero is not a valid Network ID. It will be necessary to assign the zone to one of the Network IDs defined on the Connect Plus CPS Networks screen prior to saving, writing, or cloning the codeplug.

3. **Create (or Open) a Network Frequency File for each Network ID that has been assigned to a zone**. The third major step to configuring a single SU for multiple Networks is to create or open a separate Network Frequency File for each Network ID that is defined on Connect Plus Networks screen. Without

the network frequencies, the Connect Plus radio will not be able to use the network! There are several important things to know for managing multiple Frequency Files for a single radio:

a. Prior to displaying any Network Frequency File, Connect Plus CPS must first display an Option Board codeplug (either by opening a saved codeplug or by “reading” the Option Board codeplug). Once this occurs, there are several ways to display a Network Frequency File; (a) create a new Frequency File, (b) open a saved Frequency File, or (c) read the Frequency Files from a connected radio using the *Device→Read→Frequencies* command.

b. A Connect Plus radio can store up to **16** Network Frequency Files (one per Network ID defined on the Connect Plus CPS Networks screen), but each Frequency File is still managed independently.

c. Each Frequency File has a Network ID field, which defines the Network ID for the Frequency File. When a new Frequency File is created, the Network ID defaults to Network ID zero (as a placeholder until the Frequency File is assigned to a network). Network ID zero is not a valid Network ID. It will be necessary to assign the Frequency File to one of the Network IDs defined on the Connect Plus CPS Networks screen prior to saving, writing, or cloning the Frequency File.

d. Each frequency file contains sites and frequencies for just one network.

e. Frequency file version numbers are managed independently for each Network. For more information on Frequency File version numbers, see section “Special Considerations for Network Frequency File”.

f. When searching frequencies, the Connect Plus Option Board only loads one Frequency File at a time. This is the Frequency File with the Network ID that matches the Network ID for the currently selected zone.

g. When using Connect Plus CPS and a programming cable, the Option Board can be programmed with any Network Frequency File that matches a Network ID defined in the Option Board codeplug. However, via over-the-air file transfer, the Option Board can only acquire the Frequency File that matches the Network ID for the site to which the radio is currently registered. The Option Board cannot acquire a Frequency File for a different Network ID over-the-air. When the Network Manager user attempts to upload a Network Frequency File to the XRC Controller for over-the-air transmission, the Network Manager software checks whether the Network ID in the Frequency File matches the Controller’s Network ID. If they do not match, the file upload is denied and Network Manager provides an error message.

h. When saving frequency file information to a file archive, each Frequency File can be saved independently, or multiple Frequency Files can be saved in a single “Multi-Network Frequency File”. For more information, see the MOTOTRBO Connect Plus CPS Help file.

i. When the Connect Plus CPS user utilizes the *Device→Read→Codeplug* command or the *Device→Read→Frequencies* command, this will automatically clear any Frequency File that is currently being displayed on the Connect Plus CPS screen. If desired, save the displayed Network Frequency File(s) to disk prior to issuing these commands.

j. When opening frequency file information from archived files with Connect Plus CPS, each Frequency File can be opened independently (if saved in the .tfn file format), or multiple Frequency Files can be displayed by opening a single file (if saved in the .mnf file format). For more information, see the MOTOTRBO Connect Plus CPS Help file.

    i. When opening a previously saved Frequency File, Connect Plus CPS checks to make sure that the Frequency File frequencies match the frequency band supported by the displayed codeplug. If not, an error message is returned.

ii. If the Network ID in the Frequency File that is being opened matches the Network ID for a Frequency File already displayed on the screen, the Frequency File that is being opened will replace the currently displayed Frequency File.

iii. If the Frequency File that is being opened has a Network ID that is not defined on the Networks Screen of the currently displayed codeplug, Connect Plus CPS will still open and display the Frequency File (provided that certain checks are passed), but it automatically changes the Network ID to zero when displaying the file. This serves as a placeholder until the Frequency File is assigned to a valid network. It will be necessary to assign the Frequency File to the one of the Network IDs defined on the Connect Plus CPS Networks screen prior to saving, writing, or cloning the Frequency File.

k. Connect Plus allows the user to save and open multiple frequency files as *Multi-network Frequency files* (*.mnf) file type. When opening a previously saved Multi-network Frequency files, Connect Plus CPS verifies that each Frequency File frequencies match the frequency band supported by the displayed codeplug. If not, the Frequency file of the corresponding network ID will not be opened and an error message is displayed. Connect Plus CPS will close all displayed Frequency Files when opening *Multi-network Frequency files* (*.mnf). Note that for OTA programming, each Frequency File must be saved independently – *Multi-network Frequency files* cannot be used with the OTA file transfer feature.

Important! Connect Plus enforces a correlation between the Network IDs defined in the Option Board codeplug and the Network Frequency Files that the Option Board will store. Precedence is given to the Network IDs defined in the Option Board codeplug.

- The Connect Plus Option Board will not accept a Frequency File if the Network ID in the Frequency file is not defined in the Option Board's current codeplug.

- Whenever the Option Board codeplug is updated, the Option Board checks the Network IDs supported by the code*plug with the Network IDs in* its currently stored Network Frequency Files. If the Option Board has any Network Frequency *File containing a Network ID* that is not defined in its codeplug, the Option Board automatically deletes that Frequency File. This operation assures that the Option Board will always have room for Frequency Files with Network IDs that are supported by its codeplug.

- When Reading frequency information from the Option Board, the Connect Plus CPS user can read all Frequency Files in the Option Board with a single *Device→Read→Frequencies* command, but only if the Network IDs in the Option Board Frequency Files are defined on the Networks Screen of the currently displayed codeplug. If not, Connect Plus CPS provides an error message that explains the problem and alternatives for correcting the mismatch. The problem must be corrected prior to Reading the Option Board's Frequency Files.

- When Writing or Cloning frequency information to the Option Board, the Connect Plus CPS user can Write or Clone all Frequency Files currently displayed on the screen with a single *Device→Write→Frequencies* command (or a *Device→Clone→Frequencies* command), but only if the Network IDs in the displayed Frequency Files are defined in the Option Board's current codeplug. If not, Connect Plus CPS provides an error message that explains the problem and alternatives for correcting the mismatch. The problem must be corrected prior to Writing (or Cloning) the Frequency Files currently displayed on the screen.

Figure 2-14 depicts a Connect Plus radio that has been programmed to use three different Networks. In this example, the Network IDs are "A", "B", "C" for simplicity. In actual practice, a Network ID is represented with a number between 1 and 4095, not a letter.

In this example, when the radio user wants to use Network A, he/she will select Connect Plus Zone 1. As long as Zone 1 remains selected, the radio will only use Network A, and it will only load the Frequency File for Network A. If the radio user wants to use Network B, he/she must select Connect Plus Zone 2. After selecting Connect Plus Zone 2, the radio will load the Frequency File for Network B and begin searching the Network B site(s). If the radio user wants to use Network C, he/she must select Connect Plus Zone 3. After selecting Connect Plus Zone 3, the radio will load the Frequency File for Network C and begin searching the Network C site(s).

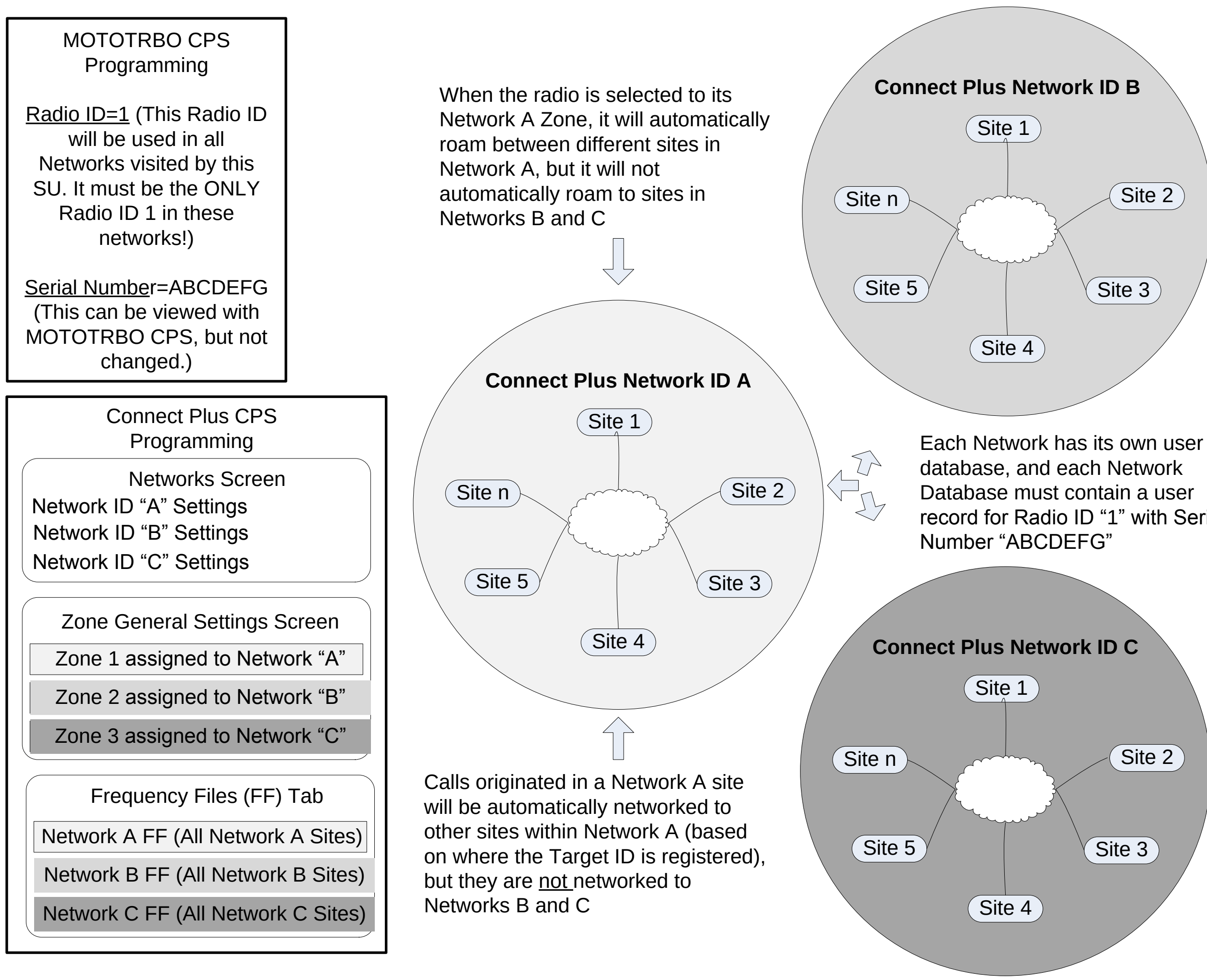


Figure 2-14 Multiple Connect Plus Network IDs

2.15 Programmable Range for Connect Plus IDs

The programmable ID range is Connect Plus is slightly less than Digital MOTOTRBO Conventional (which supports entries up to 16776415). In Connect Plus, the highest configurable ID is 16776351.

The Connect Plus software will use the same Radio ID that is programmed with MOTOTRBO CPS. Although MOTOTRBO CPS allows the entry of Radio IDs 16776352 through 16776415, these numbers must not be used for Connect Plus radios. If any of these numbers is used as the Radio ID, the SU will not function correctly in the Connect Plus personality until the number is changed to a Radio ID that falls within the allowable Connect Plus range. Connect Plus supports the following ranges:

- The programmable range for Radio IDs (Unit IDs) is 1-16776351
- The programmable range for Group Call IDs and Multigroup Call IDs is 1-16776351. Any number from this range can be used as a regular Group Call contact type, or as a Multigroup Call contact type, but the same number cannot be used for both.
- The programmable range for Dispatch Call IDs is 1-16776351
- Site All Call (voice) uses a fixed ID of 16777215. This cannot be changed by the user.
- Site All Call (text) uses a fixed ID of 16776415. This cannot be changed by the user.

2.16 Connect Plus Voice and Data Privacy

Privacy refers to the ability to send and receive encrypted communications, providing security that goes beyond the normal signaling protocol. When discussing Enhanced Privacy, an encrypted transmission is also called “protected”, “scrambled”, or “secure”. An unencrypted transmission is also called “unprotected”, “unscrambled”, or “clear”.

In Connect Plus, protected transmissions are encrypted/decrypted by the MOTOTRBO SU, using the **Enhanced Privacy** feature. For this reason, the reader should be familiar with the extensive description of MOTOTRBO Enhanced Privacy provided in Reference [1]. Much of that information also applies to Connect Plus and will not be repeated here. Instead, this section will highlight some important differences between Privacy operation in Connect Plus and other MOTOTRBO modes, and it will discuss some important Privacy considerations for Connect Plus.

Briefly stated, the most important differences between Privacy in Connect Plus and other MOTOTRBO digital modes are as follows:

- Connect Plus supports only Enhanced Privacy. It does not support Basic Privacy.
- Currently, Connect Plus Enhanced Privacy is for voice transmissions only. At the present time, Connect Plus IP datagrams (location updates, text messages, etc) are always transmitted unprotected. It should also be noted that CSBK messages are always sent unprotected (just as in all other MOTOTRBO digital modes).

- While voice encryption/decryption is done by the MOTOTRBO SU, the Connect Plus Option Board plays a critical role in enabling/disabling Enhanced Privacy, in determining which Privacy Key ID the radio uses for a protected transmission, and in showing the user whether a received voice transmission is protected or unprotected. In order for Enhanced Privacy to work correctly in Connect Plus, the SU must be properly configured with both MOTOTRBO CPS and MOTOTRBO Connect Plus CPS.

Types of Privacy

Connect Plus supports Enhanced Privacy only. Basic Privacy is not supported.

If Privacy is desired for a Connect Plus SU, its radio-wide Privacy Type must be set to “Enhanced” with MOTOTRBO CPS.

If Enhanced Privacy will be utilized in the Connect Plus network, then each repeater utilized by Connect Plus (network wide) must be configured for “Enhanced” Privacy Type using MOTOTRBO CPS. Although Enhanced Privacy may sometimes appear to work correctly when not enabled in the repeater, proper configuration of the repeater’s Enhanced Privacy setting is essential for consistent and reliable operation.

Strength of the Protection Mechanism

Because encryption/decryption is done by the MOTOTRBO SU, refer to the section entitled “Strength of the Protection Mechanism” in Reference [1].

2.16.1 Scope of Protection

In Connect Plus, Enhanced Privacy can be enabled/disabled per position on the Channel Selector Knob or Channel Rocker (depending on radio model).

When enabled for a Connect Plus channel position, the radio will encrypt all voice transmissions made while the radio is selected to that position. This includes the following:

- Non-emergency voice transmissions for the Selected Group ID (this can be a regular Group, Multigroup, or Site All Call).
- Emergency voice transmissions for the Selected Group ID or Emergency Revert Group ID (this can be a regular Group or Multigroup).
- If the radio scans into a voice call, and if the radio user presses PTT to talk back during Call Hang Time, the voice transmission will be protected using the Key ID for the selected channel position. Note: Talkback is not allowed for Site All Call and non-emergency Multigroup Call.
- Private Call Voice Transmissions. The transmission will be protected using the Key ID for the selected channel position.
- Remote Monitor Voice Transmissions. The transmission will be protected using the Key ID for the selected channel position.

2.16.2 Effects on Performance

Refer to the section entitled “Effects on Performance” in Reference [1].

Privacy and Connect Plus System Components

This section briefly states the interaction of the Enhanced Privacy feature with various system components.

MOTOTRBO SU: The MOTOTRBO SU takes the primary role for encrypting/decrypting transmissions. See the next section for a further discussion of the MOTOTRBO CPS programmable Privacy settings.

MOTOTRBO Repeater: Enhanced Privacy must be enabled as the radio-wide Privacy Type using MOTOTRBO CPS.

Connect Plus Option Board: Various Privacy Settings must be enabled using MOTOTRBO Connect Plus CPS, and some of these must align with the Privacy settings configured with MOTOTRBO CPS. See the next section for a further discussion of the Connect Plus CPS programmable Privacy settings.

XRC Controller: The XRC does not currently have any configurable Privacy settings, nor does it have the ability to encrypt or decrypt protected transmissions. Voice Privacy is encrypted by the transmitting SU and decrypted by the receiving SU. To the XRC, it is just a “pass through”. The XRC routes both types of voice transmissions (protected and unprotected) based on the IDs used in the transmissions.

Third-party data applications: All IP datagrams between the Connect Plus System and third party data applications are sent unprotected.

XRT Controller Gateway & XRT Clients: The XRT Controller Gateway does not currently have any configurable Privacy settings, nor does it have the ability to encrypt or decrypt protected transmissions. The XRT routes audio to/from its Clients based on the IDs used in the transmission. The XRT is not aware of whether the audio that is being routed is protected or unprotected. When protected audio is routed to a XRT Client, it will be intelligible to the Client application’s end user provided that (a) the Client application supports MOTOTRBO Enhanced Privacy, and (b) the Client application has been configured with the same **Key ID**/**Key Value** pair as the device that is transmitting the protected audio stream.

Wireless Consoles: Because a Wireless Console (such as the MC1000, MC2000, or MC2500 Deskset Console) connects via a Connect Plus mobile radio, it is able make and receive protected voice transmissions. The encryption/decryption is performed by the radio, and not by the console. However, since the mobile radio is not usually in the same location as the console operator, the console operator may not be enable/disable Enhanced Privacy “on the fly” via a programmable button or menu option. (The MC Series Deskset Consoles does not have this capability). However, the console operator can make both protected and unprotected transmissions to the same Group ID, provided that the same Group is assigned to two different channel positions with Connect Plus CPS – one with Privacy enabled and one with Privacy disabled. The console operator can then select the desired position via the Channel Select feature.

2.16.3 MOTOTRBO CPS Configuration

It is important to understand the inter-relationship between the SU's programmable Privacy Settings in MOTOTRBO CPS and MOTOTRBO Connect Plus CPS.

Privacy Screen

- Radio-wide Privacy Type must be set to "Enhanced"

- The SU's Privacy Table must be configured with each Key ID, Key Alias, and Key Value that will be used by this SU:

    - All Key ID/Key Values pairs that the SU will use while sending or receiving an encrypted transmission must be defined on this table.
      The table supports a total of 16 entries.

    - Any and all Key IDs that will be configured in the radio's Connect Plus CPS codeplug must be defined on this table. Failure to follow this rule constitutes a key mismatch and will likely result in an operational error (i.e. failure to encrypt and/or decrypt a transmission).

    - The Key Alias field is not used by Connect Plus and can be left with the default alias (or aliases).

Buttons Screen

- Configuring a Privacy On/Off button with MOTOTRBO CPS has no effect on Connect Plus operation, but is helpful if the same radio is also used for non-Connect Plus digital modes.

Menu Screen

- Enabling the "Privacy" Utilities Menu option with MOTOTRBO CPS has no effect on Connect Plus operation, but is helpful if the same radio is also used for non-Connect Plus digital modes.

Privacy settings per digital channel

- Do not check the Privacy checkbox with MOTOTRBO CPS for Connect Plus channels. This setting will be automatically enabled/disabled by the Connect Plus Option Board behind-the-scenes.

- Do not set the Privacy Alias (on the Digital Channel screen) with MOTOTRBO CPS. This will be automatically set by the Connect Plus Option Board behind-the-scenes.

2.16.4 MOTOTRBO Connect Plus CPS

General Settings Screen

- Check the box labeled, "Enable Privacy Settings"

Buttons Screen

- Configuring a Privacy On/Off button with Connect Plus CPS allows the user to toggle Enhanced Privacy On or Off for each position on the Channel Selector Knob or Channel Rocker (depending on radio model). The Connect Plus Option Board tracks the Privacy setting (on/off) separately for each position.

Menu Screen

- Enabling the Privacy Utilities option allows the user to toggle Enhanced Privacy On or Off via the menu for each position on the Channel Selector Knob or Channel Rocker (depending on radio model). The Connect Plus Option Board tracks the Privacy setting (on/off) separately for each position.

Zone Channel Selections Screen

- There is a checkbox labeled "Privacy" for each channel position. Check the box to enable Privacy for the corresponding position when writing the Connect Plus codeplug to the radio. Uncheck the box to disable Privacy for the corresponding position when writing the Connect Plus codeplug to the radio. It is important to note that this setting can be changed by the radio user if a Privacy on/off button or Privacy Utilities Menu option has been programmed with Connect Plus CPS. Therefore, if the box is enabled when writing the Option Board codeplug to the radio, the radio user can disable the setting via the Privacy button or Menu option. If the box is disabled when writing the Option Board codeplug to the radio, the radio user can enable the setting via the Privacy button or Menu option.

- For each channel position there is a field labeled "Key ID", which can be configured with value of 1-255. This value determines which Key ID (and, indirectly, which Key Value) the radio uses while transmitting if Privacy is enabled for the selected channel position. <u>It is critical to note that any Key ID value configured on this screen must also be configured in the SU's Privacy Table with MOTOTRBO CPS. Failure to do so results in a programming mismatch and the Connect Plus Enhanced Privacy feature will not work!</u>

2.16.5 User Control Over Privacy

Connect Plus CPS allows the enabling or disabling of Enhanced Privacy for each selected channel position.

The option to toggle the privacy capability per channel position can additionally be given to the radio user by using Connect Plus CPS to provide a menu option or programmable button. Without the menu option or programmable button, the radio user is essentially "locked" to the privacy setting as programmed with Connect Plus CPS.

It is important to note that if the radio user is provided with the menu option or programmable button, and if he/she toggles the privacy setting, only the selected position's privacy setting is toggled (and remains toggled even after the user changes to a different position or zone). Toggling the privacy setting for a specific channel position will not affect the privacy setting for a different channel position.

If the decision is made to allow the radio user to toggle the Privacy setting on and off, this can be accomplished via either the programmable Privacy on/off button or the Privacy menu option. However, providing a programmable Privacy on/off button has some advantages over providing the programmable menu option:

- The programmable button is available to all radios, whereas the programmable menu option is only available to display radios.

- There are some scenarios in Connect Plus where the radio user is temporarily prevented from using the menu, but the programmable button is usually still accessible.

The radio settings for "All Tones" and "Keypad Tones" must both be enabled (i.e "on") for the radio user to hear all of the Enhanced Privacy tones discussed in the following paragraphs.

When the radio user toggles Privacy On with the programmable button, the radio plays a tone that rises in pitch. A display-equipped radio also briefly displays a confirmation message, when possible. There are some instances where the confirmation message won't be shown because the display is already occupied with other important information. However, the tone is still played.

When the radio user toggles Privacy Off with the programmable button, the radio plays a flat tone. A display-equipped radio also briefly displays a confirmation message, when possible. There are some instances where the confirmation message won't be shown because the display is already occupied with other important information. However, the tone is still played.

When changing the Privacy state with the Menu option, the radio provides a confirmation message, but not the ascending or descending tone.

It should be noted that a Connect Plus radio must be currently registered to a site in order for the user to toggle the Privacy setting for the selected channel position. The radio user cannot toggle the Privacy setting via the programmable button or the menu while the radio is searching for a site.

When Privacy is enabled for the selected channel position, this controls whether the radio will transmit protected voice when PTT is pressed. This does not affect whether the radio will receive a protected transmission. When enabled for Enhanced Privacy with MOTOTRBO CPS, the radio always tries to decrypt protected transmissions -- regardless of whether Privacy is currently enabled or disabled for the selected channel position. In addition, it is possible for two radios to successfully communicate when they are both encrypting, but transmitting with different Keys. If the Key ID/Key Value pair used in the transmission resides anywhere in the Privacy Table of the receiving radio, it will successfully decrypt the transmission. If not, the received audio will be garbled or muted, depending on the specific key mismatch scenario. If a radio is not supposed to decrypt a protected transmission, do not program that Key ID/Key Value pair into the radio's Enhanced Privacy table.

2.16.6 Privacy Indications to User

It is important for a radio user to know the privacy status (i.e. enabled or disabled) of the currently selected channel position, and also to know if the received voice transmission is unprotected or a protected voice transmission.

Privacy Icon

The Privacy icon is a padlock, with two variations; open padlock and closed padlock.

When a display-equipped radio is correctly configured for Enhanced Privacy with both MOTOTRBO CPS and Connect Plus CPS, it displays a Privacy icon while idle and during a call as discussed below:

1. When the radio is idle (not in a call), the Privacy icon displays at the top of the Home Screen, about 3/4 of the way to the right-hand side of screen:
    a. The open padlock icon indicates that transmit Privacy is currently disabled for the selected channel position.
    b. The closed padlock icon indicates that transmit Privacy is currently enabled for the selected channel position.
2. When the radio is in a voice call, the Privacy icon displays on the far right-hand side of the top line.
    a. While transmitting voice:
        i. The open padlock icon indicates that the transmission is unprotected.
        ii. The closed padlock icon indicates that the transmission is protected.
    b. While receiving a voice transmission:
        i. Steady (not flashing) open padlock icon: The transmission that is currently being received is unprotected. If the radio user presses PTT in order to talk back, his transmission will also be unprotected (because Transmit Privacy is currently disabled.)

ii. Flashing open padlock icon: This indicates a mismatch in the Privacy state of the sender and receiver. The transmission that is currently being received is unprotected. However, if the radio user presses PTT in order to talk back, his transmission will be protected (because Transmit Privacy is currently enabled.)

iii. Steady (not flashing) closed padlock icon: The transmission that is currently being received is protected. If the radio user presses PTT in order to talk back, his transmission will also be protected (because Transmit Privacy is currently enabled.)

iv. Flashing closed padlock icon: This indicates a mismatch in the Privacy state of the sender and receiver. The transmission that is currently being received is protected. However, if the radio user presses PTT in order to talk back, his transmission will be unprotected (because Transmit Privacy is currently disabled.)

The absence of the Privacy icon on a display-equipped radio indicates that Enhanced Privacy has not been configured (or has not been configured correctly) in MOTOTRBO CPS, Connect Plus CPS, or both.

Inconsistent display of the Privacy icon (in other words, the Privacy icon is seen during some call states, but not others) also indicates a configuration error. For more information, see the sub-section called, “Configuration Mismatches”.

LED Operation

Upon receiving a voice transmission, the radio user can know the privacy status of the voice transmission by observing the blinking rate of the receive LED. When receiving an unprotected voice transmission, the LED flashes green at a steady rate. When receiving a protected voice transmission, the LED flashes green in a specific pattern (flash, flash, pause, flash, flash, pause, etc.)

Note: Whenever the radio receives a protected call, the LED flashes green in the pattern described above. This is even true when the radio can’t decrypt the call because it is not enabled for Privacy, and when the radio is enabled for Privacy but is not configured (or correctly configured) to decrypt the call.

Talk Permit Tone

When the radio user presses PTT to begin a voice transmission, the Talk Permit Tone (if enabled through radio programming) sounds slightly different depending on whether Privacy is currently enabled or disabled for the selected channel position. When Privacy is enabled, the Talk Permit Tone is slightly lower in pitch.

Non-Display/Numeric Display radios

Radio users with non-display or numeric display radio models are not able to view the Privacy icon. Therefore, it is recommended that such users should not have the option to toggle the privacy setting. If they are provided with this option via a programmable Privacy on/off button, the only indication about whether they are toggling Privacy on or off will be tone that is played when the Privacy setting is toggled.

If non-display or numeric display radio users must be able to toggle between protected and unprotected, it is recommended that this be done by programming the same Talk Group for more than one channel position. One position would have Privacy permanently enabled, and the other position would have Privacy permanently disabled. The user can then select the appropriate channel position to determine whether transmit Privacy should be on or off. It is important to remember that the selected position determines not only the Privacy setting for the selected Talk Group, but also for any voice transmission made while selected to that position.

2.16.7 Enhanced Privacy and Emergency Calls

If a radio user presses the Emergency On button to initiate an Emergency Call, whether his/her voice transmissions will be sent unprotected or protected during the Emergency Call depends on the Privacy state of the currently channel position. If Privacy is enabled for the selected channel position when the Emergency button is pressed, the radio's Emergency voice transmissions will be protected, using the Privacy Key ID for the selected channel position. If Privacy is disabled for the selected channel position when the Emergency button is pressed, the radio's Emergency voice transmissions will be unprotected. The Emergency initiator cannot change the Privacy state of his/her radio during the Emergency Call. The Privacy state that is in effect when the Emergency button is pressed will be in effect for the duration of that Emergency Call. This rule only applies to Emergency initiators. An Emergency receiver can toggle the Privacy state of his/her radio to match the Emergency initiator (provided that the Emergency receiver has not pressed the Emergency On button on his/her radio also).

Because the Privacy state of an Emergency Call follows the selected Channel position, and because the radio user cannot always predict what channel position will be selected when he/she has an emergency, the following configuration guideline is strongly recommended: If a person is expected to receive Emergency Calls, to understand them, and to appropriately respond to the emergency, then his/her radio must be programmed (via MOTOTRBO CPS) with the same Key ID/Key Value pairs as the initiating radio. Following this rule assures that the receiving radio will be able to decrypt the initiating radio's voice transmission, no matter which channel position is currently selected on the initiator or receiver.

2.16.8 Enhanced Privacy and Remote Monitor

The Remote Monitor feature allows an authorized user to activate a target radio's microphone and transmitter for a period of time. A call is silently set up on the target radio, and its PTT is activated remotely without any indications given to user of the transmitting radio. The duration that the target radio transmits after receiving a Remote Monitor command is set in the target radio through Connect Plus CPS programming.

Whether the target radio sends its Remote Monitor voice transmission unprotected or protected depends on the Privacy state of its currently selected channel position when the radio receives the Remote Monitor command. If Privacy is enabled for the selected channel position, the radio's Remote Monitor voice transmissions will be protected, using the Privacy Key ID for the selected channel position. If Privacy is disabled for the selected channel position, the radio's Remote Monitor voice transmission will be unprotected. Because the radio user is not supposed to know that his/her radio is transmitting, the radio display (including the Privacy icon) will be the same as when the radio is idle and monitoring the Control Channel.

When the radio that requested the Remote Monitor receives the voice transmission, its display does not show any Privacy icon to indicate whether the received transmission is unprotected or protected. However, the radio user can tell whether the received transmission is unprotected or protected by looking at the radio's LED. See the sub-section "LED Operation" for more information.

It is important to note that if the transmitting radio is sending protected voice, the receiving radio must have the same Key ID/Key Value pair used for the transmission defined in its MOTOTRBO CPS Privacy Table. If not, the transmission will be garbled or muted, depending on the specific Privacy mismatch scenario.

2.16.9 Mismatches in Privacy States of Transmitting and Receiving radios

If two radios are participating in a call, and if Privacy is enabled for the channel position in one radio but disabled in the other radio, the radios are still able to communicate (provided they have the same Privacy Key information). However, the transmissions are protected in only one direction. Only the transmissions from radios with privacy enabled are protected.

It is generally recommended that all call participants transmit in the same way – either unprotected or protected. If the radio has been programmed with a Privacy on/off button, the user can enable or disable privacy for the selected channel position during a call-in-progress, provided that the radio is not currently transmitting. There is one exception to this rule. The initiator of an Emergency Call is locked into the transmit Privacy setting in effect when the Emergency On button was pressed for the duration of the Emergency Call.

The two major considerations for configuring Enhanced Privacy for Connect Plus are:

1. When setting up an individual radio for Enhanced Privacy, the SU must be correctly configured with both MOTOTRBO CPS and Connect Plus CPS before the feature will operate properly.

2. When setting up multiple radios to communicate with each other using Enhanced Privacy, the radios must be programmed with the same Key IDs and Key Values on their Privacy Table. The Key ID/Key Value pair used for the protected transmission must exactly match with a Key ID/Key Value pair programmed into the receiving radio.

Some possible configuration errors (and their associated indications) are discussed below:

- Enhanced Privacy settings are not configured with MOTOTRBO CPS, and are also not configured with Connect Plus CPS: No Privacy icon (open or closed padlock) displays at any time. **Note**: This is the normal condition for radios that do not wish to use the Enhanced Privacy feature.

- Enhanced Privacy settings are not configured with MOTOTRBO CPS, but are configured with Connect Plus CPS: No Privacy icon (open or closed padlock) displays at any time. On the Connect Plus CPS General Settings screen, “Enable Privacy Settings” is checked when writing the Connect Plus codeplug to the radio, but is “unchecked” when reading back the Connect Plus codeplug back from the radio.

- Enhanced Privacy settings are configured with MOTOTRBO CPS, but not with Connect Plus CPS. The radio will not transmit a protected call. However, the radio will be able to decrypt a protected call if the transmitting radio uses a Key ID/Key Value configured in the receiving radio. If the radio receives an unprotected or a protected call (regardless of whether the call is successfully decrypted), a blinking closed padlock icon displays while receiving the transmission. However, the icon may not be displayed consistently indicating a configuration mismatch between main radio codeplug and OB codeplug. No Privacy icon displays while transmitting, or while the radio is idle.

- User enables Privacy and presses PTT, but the Privacy Key ID programmed with Connect Plus CPS for the selected position does not exist on the Privacy Table programmed with MOTOTRBO CPS (in the same radio). Indication: The Privacy icon shows as closed padlock while idle, but changes to open padlock when user presses PTT. (Normally, it would show as a closed padlock while idle and as a closed padlock after pressing PTT.)

- LED indicates that radio is receiving a protected transmission (see sub-section called “LED Operation”), but the speaker audio is muted or garbled. This can indicate one of the following conditions:

    - Receiving radio is not enabled for Enhanced Privacy[23]
    - Receiving radio is enabled for Enhanced Privacy, but the radio is not decrypting the transmission for one of the following reasons:
        - The transmitting radio is using a Key ID not defined in the receiving radio[23]
        - The transmitting radio is using a Key ID that is defined in the receiving radio, but is paired with a different Key Value than used by the transmitting radio.[24]

[23] These may not be error conditions at all. Both radios may be correctly configured, and the receiving radio is not intended decrypt the received transmission.

2.16.10 Keys and Key Management

For Connect Plus Enhanced Privacy, both the Key ID(s) and the Key Value(s) must be programmed into the SU's Privacy Table using MOTOTRBO CPS. The Key ID is configured as a decimal value (1 – 255) and the Key Value is configured as a hexadecimal value (1 – FFFFFFFFFE). The MOTOTRBO CPS rules for displaying keys in saved codeplug files and cloning keys from one codeplug file to another are discussed in the "Keys and Key Management" section of Reference [1]. That section also addresses strategies for changing the Keys programmed into the radio's Privacy Table with MOTOTRBO CPS. This may be necessary if the Privacy Keys are compromised in some fashion.

As previously discussed, a radio can decrypt a protected transmission if the receiving radio has exactly the same Key ID/Key Value match in its Privacy Table.

Example A:

> Transmitting radio encrypts transmission using Key ID 1, which is paired with Key Value "A".
>
> The receiving radio has Key ID 1 programmed on its Privacy Table, and Key ID 1 is paired with Key Value "A". This is an exact match, and speaker audio is intelligible on the receiving radio.

Example B:

> Transmitting radio encrypts transmission using Key ID 1, which is paired with Key Value "A".
>
> The receiving radio has Key ID 1 programmed on its Privacy Table, and Key ID 1 is paired with Key Value "B". This is not an exact match, and speaker audio is garbled on the receiving radio.

It is important to note that Connect Plus has a critical Key Management rule that does not exist in other MOTOTRBO digital modes. The rule is as follows:

Once a Key ID (1 – 255) is used anywhere in the Connect Plus Network, any Connect Plus SU (in the same network) that is programmed with this same Key ID must be programmed with exactly the same Key Value to match. Here is an example of a violation of this rule:

> Eddie's Ambulance service is programmed to use Key ID 1, which is paired with Key Value "A". Francine's Florist Delivery, another company in the same network, is programmed to use Key ID 1, which is paired with Key Value "B". Even though these two companies will never talk to one another, this is a violation of this critical rule, and must be avoided. Instead, program the radios from Francine's Florist Delivery to use a Key ID that is not used by any other company, network wide. This assumes that Francine's Florist doesn't need to communicate with other companies using protected transmissions. If two or more companies desire to communicate with one another using protected transmissions, the radios must be programmed with same Key ID(s) and Key Value(s).

Although the above rule is not enforced by the system software, failure to follow this rule in the present will likely make it necessary to reprogram some radios in the future. This is because a future version of XRC software may support a programmable Enhanced Privacy Table for the controller. This will be necessary to support protected IP datagrams (location updates, text messages, etc) in the Connect Plus network. When and if this occurs, the XRC Privacy table will support just one Key ID to Key Value relationship network-wide. Any SU that is programmed with a different Key ID to Key Value Relationship than what is programmed into the controller will not be able to received protected datagrams. This rule implies that every Connect Plus network, even networks with multiple customers, should have a single individual to manage Privacy keys network wide.

---

[24] This configuration mismatch must be avoided in Connect Plus. For more information, see section "Keys and Key Management".

If a Connect Plus radio will be utilizing Enhanced Privacy on multiple Connect Plus Networks (in other words, the radio is configured to use Multiple Network IDs), the following points should be considered carefully:

- The Privacy Table in the SU supports sixteen total entries. The Privacy Key ID/Key Values that the SU will use (transmit and/or receive) in all networks must be defined in these sixteen entries.

- The design of the SU's Privacy Table necessitates coordination/communication between the administrators of the different networks. For example, the SU cannot use Key ID 1 in multiple networks, unless Key ID 1 is paired with the same Key Value in all of those networks.

Data Gateway Privacy Settings

Connect Plus does not currently support Enhanced Privacy for IP datagrams (such as Location Updates and Text Messages). This includes IP datagrams passed between 3rd party applications and the Connect Plus System. The information contained in the section entitled "Data Gateway Privacy Settings" in Reference [1] does not apply to Connect Plus.

2.17 Connect Plus RDAC Interface

Repeater Diagnostics and Control (RDAC) software can be used in the Connect Plus system to monitor and control repeaters on a Connect Plus site. The RDAC configuration and capabilities for Connect Plus are similar to IP Site Connect mode.

There are several important points to note regarding RDAC operation in a Connect Plus system:

- When using RDAC with Connect Plus, the RDAC application must be configured for "IP Site Connect Mode". For Connect Plus, each "IP Site Connect System" equates to one Connect Plus site. Earlier versions of RDAC supported just one IP Site Connect System (i.e. one Connect Plus site) per instance of the RDAC application. Newer versions of RDAC can communicate with more than one IP Site Connect Master. This means that newer versions of RDAC can be configured to monitor multiple IP Site Connect Systems (i.e. multiple Connect Plus sites) from a single instance of the RDAC application. However, any Connect Plus site managed by the RDAC application (whether a single Connect Plus site or multiple Connect Plus sites) must reside in the same LAN or VPN as the PC running the RDAC application.

- When configuring the RDAC application, the controller's IP address and port is set as "Master". RDAC communicates with the controller in order to obtain IP addresses for the site's repeaters. Once RDAC has a repeater IP address, it can communicate with that repeater directly.

- The PC hosting the RDAC application must be on the same Local Area Network (LAN) or Virtual Private Network (VPN) as the controller and the site's repeaters. The reason is as follows: RDAC communicates with the XRC and with the site's repeaters via the Link Establishment (LE) Protocol. The Controller is the LE Master and the repeaters and RDAC are LE Peers. If Peers are ever located in different networks, then <u>all</u> peers must address the Master via its publicly addressable IP, not its local IP address. This even applies to the peers that are in the same LAN as the Master. This requires a router capable of a special feature called "hair-pinning", which turns the messages around to send them back to the Master (in this case, the XRC controller). Due to the time sensitive nature of the messaging between the XRC controller and its peer repeaters, the latency added by this additional routing and the hair-pin address conversion will be detrimental to system performance. For this reason Connect Plus requires all Peers, including RDAC, to be located in the same Local Area Network (LAN) or Virtual Private Network (VPN) as the XRC controller acting as Master. Only a single RDAC instance is supported per site (per Master/XRC).

- When configuring the RDAC application, set the RDAC ID[25] for a value higher than 15. This assures that there will be no conflict with a Radio ID that might be already programmed into one of the site's repeaters. (In Connect Plus, each site repeater is programmed for a unique Radio ID between 1 and 15.)

- The XRC has a configurable parameter called "RDAC UDP Listen Port". This field, which appears on the MOTOTRBO Connect Plus Network Manager Site Configuration screen, determines which port the controller listens to for incoming messages from the RDAC application.

- When RDAC sets a repeater for "Disable", the XRC controller will not use the repeater for Control Channel signaling or call assignment.

[25] ID **123** is reserved and cannot be used as RDAC ID.

2.18 Remote Repeater Programming

Remote Repeater Programming (RRP) is also called IP Repeater Programming. IP Repeater Programming is a MOTOTRBO CPS purchasable feature which allows a system administrator to provision and to upgrade repeaters within the system utilizing the IP network. This feature can be used with Connect Plus repeaters as well. This feature is supported on repeaters equipped with a 32 MB memory running on repeater firmware version R01.07.00 or later. IP Repeater Programming allows the System Administration to remotely perform the following actions:

- Read a repeater codeplug
- Write a repeater codeplug
- Update a repeater's firmware
- Enable purchasable repeater features

The configuration and operational details for IP Repeater Programming are discussed in the MOTOTRBO CPS Help File and Reference [1]. The following paragraphs discuss how the XRC supports the feature, and how it impacts Connect Plus operation.

In order for MOTOTRBO CPS to remotely program repeaters in the Connect Plus system using this feature, several preliminary steps must be taken.

1. In the repeater codeplug (32 MB repeaters only), check the box called "Enable IP Repeater Programming" on the MOTOTRBO CPS Network screen. This checkbox can only be enabled when using MOTOTRBO CPS and the USB programming cable. Once enabled, it can be disabled via either a USB or IP connection (after IP Repeater Programming set-up is finished).

2. Secure a feature Entitlement ID and enable the IP Repeater Programming feature in MOTOTRBO CPS. Until this occurs, the MOTOTRBO CPS "Remote" drop-down menu options are not available.

3. Using the "Remote" drop-down menu, configure necessary settings in MOTOTRBO CPS.

4. Configure the RRP UDP Listen Port in the XRC Controller(s).

5. Make sure that all necessary IP connections are in place.

MOTOTRBO CPS Setup

See the MOTOTRBO CPS Help File for a discussion of the configurable settings associated with IP Repeater Programming. One of the most important steps is to configure an "IP System" for each Connect Plus site. Prior to configuring the two settings below, you will need to know some information about your Connect Plus sites:

- Master IP Address: Enter the IP address of the site's XRC Controller (or, the IP address that will be used to reach the XRC controller if going through a firewall.)

- Master UDP Port: Enter the "RRP UDP Listen Port" as configured into the site's XRC controller (or, the UDP Port number that will be used to reach the controller's "RRP UDP Listen Port" if going through a firewall.)

- CPS ID: Note that ID range 1 – 15 and ID 123 are reserved and **cannot** be used as CPS ID.

MOTOTRBO Connect Plus Network Manager Setup

In each XRC Controller, use the MOTOTRBO Connect Plus Network Manager to configure the RRP UDP Listen Port. This defines the port on which the XRC will listen for connection requests from MOTOTRBO CPS. The XRC

allows one MOTOTRBO CPS device at a time to connect via this port. If a second MOTOTRBO CPS device should attempt to connect while the first device is still connected, the second device is ignored.

Establishing a connection to a remote repeater

Prior to remotely programming a repeater, the MOTOTRBO CPS user must first know which Connect Plus site the repeater is located at. The MOTOTRBO CPS user then initiates a remote connection to the “IP System Alias” that has been configured for that site. Following a successful connection, the MOTOTRBO CPS user can then choose which remote operation to perform (i.e. Read, Write, Update, or Activate). Upon initiating the desired operation, the user is presented with a list of “Available Devices”. These are the site repeaters on which the operation can be performed. The list references each device by Radio ID, IP Address, and UDP Port. The CPS user initiates the operation by selecting the desired device and pressing “OK”. This causes MOTOTRBO CPS to send a message to the target repeater via the XRC. When the repeater receives the message, it will establish a TCP/IP connection with the MOTOTRBO CPS. MOTOTRBO CPS uses this TCP/IP connection to perform the requested operation.

Once the TCP/IP connection is established between the repeater and MOTOTRBO CPS, this removes the device from service, and it will remain out of service until the operation is completed (or terminated) and the device subsequently re-establishes its link with the XRC. In other words, the operation disables the repeater for a period of time. The length of time that the repeater remains disabled depends on the network bandwidth and amount of data that is transferred to complete a selected operation. It is important to note that the controller does not instantly know that the targeted device has been removed from service. The repeater stops sending keep alive messages to the controller, and it takes approximately 30 seconds for the XRC to realize that the repeater is no longer present.

Impact on Connect Plus operation

It is important for the MOTOTRBO CPS user to understand the effect of Remote Repeater Programming on a Connect Plus repeater.

- <u>Performing Remote Repeater Programming on the active Control Channel causes the following effects.</u>
    - Radios that were listening to the Control Channel timeslot will go into Search and may possibly register with another site (in cases where there is overlapping coverage with another network site).
    - If there was a call-in-progress on timeslot two, the call will fail. Radios that were listening to the call will switch back to the Control Channel timeslot. When they don’t hear any messages coming from the Control Channel timeslot, they will go into Search.
    - Since it takes approximately 30 seconds for the XRC to realize the repeater is no longer present, the controller may assign a new call to the second timeslot of the Control Channel repeater in the interim. Any such call will fail.
    - Calls that were in-progress on other repeaters will continue. However, when those calls end, the radios will return to the Control Channel timeslot. When they don’t hear any messages coming from the Control Channel timeslot, they will go into Search.
    - If the site is configured for Control Channel Rollover (and if at least one of the other Control Channel repeaters is available) the XRC will roll-over to the new Control Channel after approximately 30 seconds. In the interim, the site has no Control Channel timeslot.
    - If there is no other Control Channel repeater to rollover to, the site will be without any Control Channel timeslot whatsoever until the Control Channel repeater re-establishes its link with the XRC Controller. In the meantime, if the controller is enabled for Auto Fallback operation, it will

intentionally stop communicating with the other site repeaters so that they will start sending the Connect Plus Auto Fallback Beacon. (For more information, see section "Automatic Fallback".)

- Performing Remote Repeater programming on a non-Control Channel repeater causes the following to occur:
  - Calls that were in-progress on a repeater timeslot will fail. The receiving radios will then switch back to the Control Channel repeater and timeslot.
  - Since it takes approximately 30 seconds for the XRC to realize the repeater is no longer present, the controller may assign a new call (or calls) to the absent repeater in the interim. Any such call will fail.
  - Once the XRC realizes that the repeater is absent, it will longer attempt to assign calls the repeater, but the site's call capacity will be reduced by two timeslots until the repeater re-establishes its link to the XRC. This may increase the number of calls that are placed into the Busy Queue before they are assigned to a traffic channel.

When a repeater disconnects due to Remote Repeater Programming, the controller knows that the repeater is absent (after approximately 30 seconds), but the controller does not know why the repeater is absent. If the Network Manager is connected to the site, it removes the repeater from the Real Time Display. The XRC also places a time-stamped "Repeater has disconnected" entry into the Event Log.

When the Remote Repeater Programming session terminates, the repeater will request a new Link Establishment with the controller. After completing LE, the repeater will once again be available for assigned calls, it will be added back to the Real Time Display, and the controller will place a time stamped entry into the Event Lot to show that the repeater has connected.

2.19 Connect Plus and Application Developer Program (ADP)

Motorola offers an Application Developer Program (ADP), which allows accredited third party developers to create customized applications used with specific MOTOTRBO interfaces such as Location Services, Text Messaging, etc.

In regards to Connect Plus, these MOTOTRBO ADP interfaces fall into three categories:

1. MOTOTRBO interfaces that are supported with some modifications needed for Connect Plus. (Location Service, Text Messaging Service, Presence Notification Service)
2. MOTOTRBO interfaces unique to Connect Plus. The XRT Gateway interface is an example. For more information, see the "XRT Gateway" section.
3. MOTOTRBO interfaces not currently supported in Connect Plus.

Where an interface is supported in Connect Plus, the third party developer will need to make some modifications for Connect Plus operation (as compared to how the product works in other MOTOTRBO digital modes.) These modifications are necessary due to the Connect Plus system architecture, which is quite different from other MOTOTRBO modes.

For accredited ADP developers, Motorola provides Application Developer Kit (ADK) documents to describe the protocols used to interface with the MOTOTRBO product. In addition to the applicable MOTOTRBO ADK document(s), a third party developer wishing to develop a product for a supported Connect Plus interface will

require an additional document explaining the ADK modifications required for Connect Plus. These modifications are most typically related to message addressing.

The following table shows whether specific MOTOTRBO interfaces are currently supported in Connect Plus.

Interfaces supported in Connect Plus	Interfaces not currently supported in Connect Plus
Text Messaging	Telemetry
Location Services	
Presence Notifier to Watcher (PN2W)[26]	
IP capable peripheral[27]	
Non-IP peripheral[27]	
Raw IP Data pass-through[27]	

Because the only Option Board slot is already occupied by the Connect Plus Option Board, the MOTOTRBO Option Board interface is not available to 3rd party developers in Connect Plus mode.

2.20 Connect Plus Telephone Interconnect

The MOTOTRBO Connect Plus Telephone Interconnect feature supports two types of interconnect calls:

- **Individual Telephone Interconnect Call** (also called, “Private Phone Call”). This allows half-duplex voice communication between a radio user and a phone user. This communication can be initiated from either party.
- **Talkgroup Telephone Interconnect Call**. This allows a telephone user to join or initiate a regular Connect Plus Group Call, thereby providing communication between the phone user and a group of radio users. This is half-duplex voice communication, and it can only be initiated by the phone user.

Any Connect Plus radio (with the appropriate privileges) can receive a Private Phone Call and participate in a Group call that has been initiated by (or is joined by) a phone user. At the current time, only display-equipped radios can initiate a Private Phone Call.

The figure below provides an overview of the system components for Connect Plus Telephone Interconnect. The figure is followed by a brief description of each component’s role.

[26] In Connect Plus Presence Notification services are provided by the XRC controller. The Motorola Presence Notifier application is not used or supported.
[27] Some messages and features supported in other MOTOTRBO modes are not currently supported in Connect Plus operation. For more information, contact MOTOTRBO Application Developer Program.

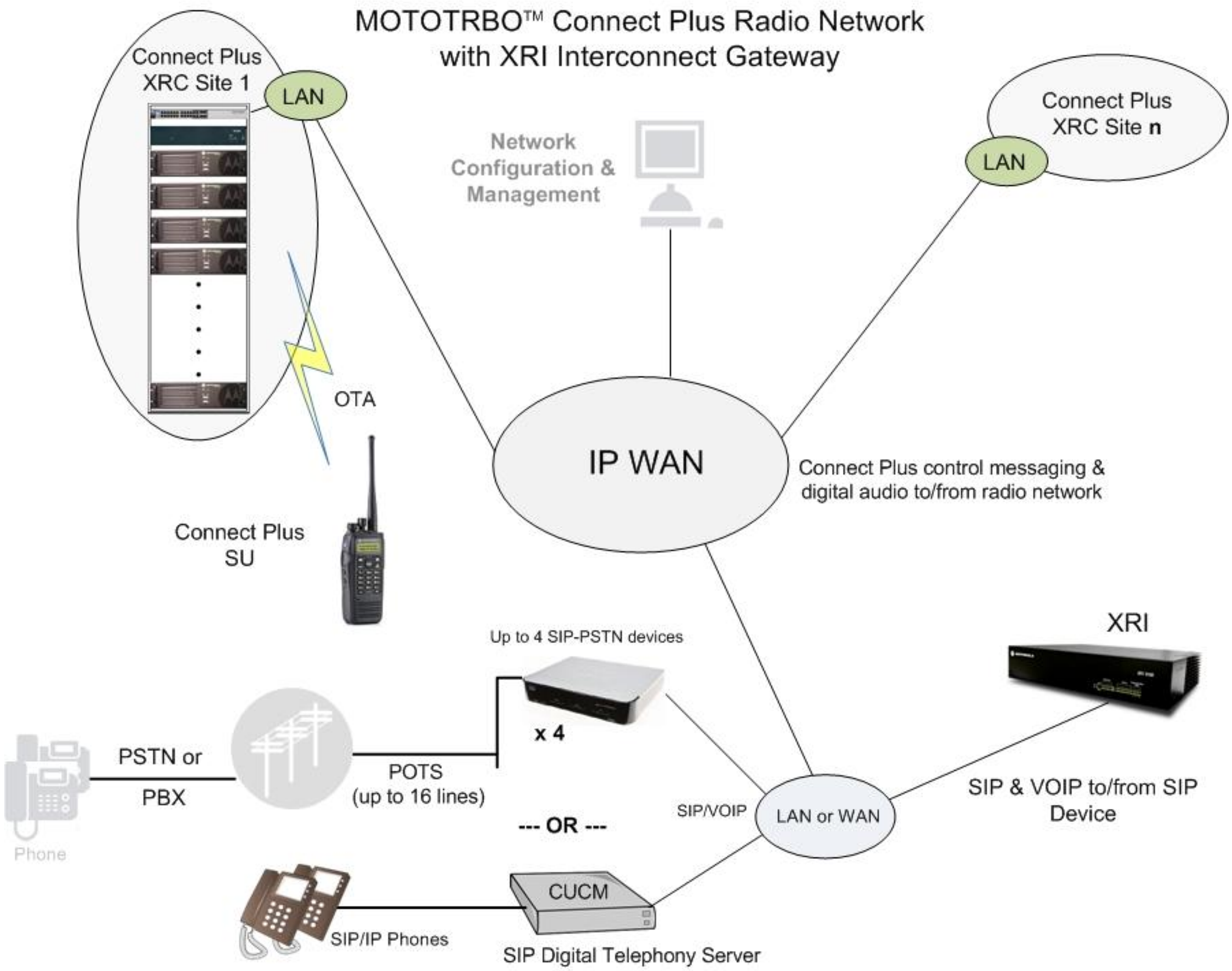


Figure 2-15 Connect Plus Telephone Interconnect Configuration

- Telephone Network: The path through which the telephone user accesses the Connect Plus system. In Connect Plus Telephone Interconnect, this can be the Public Switched Telephone Network (PSTN), or a Private Branch Exchange (PBX).

- SIP Gateway Device: Beginning with Release 1.7 (R2.6.0), the SIP Gateway Device Type to which the XRI will connect is determined by information contained in the Key Manager File which must be uploaded to the XRI, as discussed in a subsequent section. The terms used by the MOTOTRBO Connect Plus Network Manager to distinguish between the two different SIP Gateway Types supported by the XRI are (1) SIP to PSTN Gateway and (2) SIP Digital Telephony Gateway/Server.

  - **SIP to PSTN Device**: Interfaces PSTN or PBX phone lines with the IP network, and communicates with the XRI via the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP). Initially, the CISCO SPA8800 is validated as an approved SIP to PSTN device. Up to four CISCO SPA8800 devices can connect to the XRI Interconnect Gateway, and each CISCO SPA8800 can connect up to four analog phone lines via its FXO ports. These lines are sometimes referred to as PSTN (Public Switched Telephone Network) and/or POTS (Plain Old Telephone Service) lines. Alternatively, the lines may be connected to a PBX (Private Branch Exchange). This was the only SIP Gateway type supported prior to Release 1.7 (R2.6.0). XRI

Interconnect Gateway firmware prior to Release 1.7 (R2.6.0) will continue to work with the CISCO SPA8800 without uploading a Key Manager File.

- **SIP Digital Telephony Gateway**: Utilizes the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) to interface multiple SIP end points with the XRI Interconnect Gateway. This interface also supports SIP Digest Authentication when enabled and configured in both the SIP Gateway and the XRI Interconnect Gateway. The Cisco Unified Communications Manager (CUCM), formerly known as CallManager, is validated[28] as an approved SIP Digital Telephony Gateway. To work with this type of SIP Gateway, the XRI Interconnect Gateway must be enabled for either the Connect Plus SIP-10 or Connect Plus SIP-20 telephony feature license. The number in the license name indicates the number of simultaneously supported phone calls. Note: Connecting to analog phone lines may require additional hardware connected to the SIP Digital Telephony Gateway.

- XRI Interconnect Gateway: Device that provides interconnect capability by connecting the SIP Gateway Device to the Connect Plus network. When connected to a SIP to PSTN Gateway, the XRI interfaces up to 16 telephone lines to the Connect Plus network. When connected to a SIP Digital Telephony Gateway, the XRI supports up to 20 simultaneous phone calls, depending on the feature license enabled in the XRI. At the current time, Connect Plus supports one XRI Interconnect Gateway per Connect Plus radio network (i.e. per Network ID).

- XRC Controller: Interfaces the XRI to the repeaters and the Connect Plus subscriber radios.

- XRT Gateway: Interfaces the XRT Client application (such as a wireline console) to the Connect Plus subscriber radios and the XRI Interconnect Gateway. At the current time, the XRT Client application can participate in Group Calls which have a telephone user as participant. Private Phone Call (initiate or receive) is not currently supported in the XRT Gateway.

- Connect Plus MOTOTRBO subscriber radio: Mobile or portable radio that provides the radio network end point in the conversation between the radio user and the phone user.

Note: It is recommended that the SIP Gateway Devices and the XRI Interconnect Gateway be placed in the same physical location and connected to the same Ethernet switch wherever possible. This reduces that the chances that control messages between the two devices (which are sent via UDP/IP) will be dropped by routing equipment due to network impairments.

2.20.1 Key Manager File and Feature License

Beginning with MOTOTRBO Release 1.7 (R2.6.0), the SIP Gateway IP Addresses and the SIP Gateway Device Type that will be used by the XRI must be encoded in a special Key Manager File and uploaded to the XRI. The process outlined below is used for Release 1.7 (R2.6.0) and later when configuring SIP Gateway IP addresses for the first time, and must also be followed when changing (editing) the configured SIP Gateway IP addresses for the XRI. It must also be followed if upgrading from a prior release of XRI Interconnect Gateway firmware to System Release 1.7 (R2.6.0).

The configuration steps described below are performed using the MOTOTRBO Connect Plus Network Manager.

1. Obtain the Device Public Key for the XRI Device. The process is described in the XRI Interconnect Gateway User Guide.

2. Send the XRI Public Key to Motorola Solutions Customer Service along with the IP Address (or addresses) of the SIP Gateway Device(s) that will be used with this XRI. The number of IP addresses

[28] The validation has been performed with CUCM version 11.0.1.

needed varies from 1 to 4, depending on the type of SIP Gateway device that will be used. Please include the SIP Gateway device manufacturer and model name in the communication with customer service. Send the IP Address (or addresses) exactly as they should appear in the Host Address field(s) of the SIP Gateway Config tab. See the XRI Interconnect Gateway User Guide for more information.

3. Motorola Customer Service will provide a Key Manager file containing the encoded IP address (or addresses) and the SIP Gateway device type. This file must be uploaded to the XRI device as described the XRI Interconnect Gateway User Guide[29]. After uploading the file, the application user is asked to confirm the SIP Gateway device type and the IP Addresses.

4. The last step is to configure the IP Addresses (or addresses) into the Host IP Address field (or fields) on the SIP Gateway Config Tab, selecting from the IP address (or addresses) encoded in the uploaded Key Manager File. See the XRI Interconnect Gateway User Guide for more information.

2.20.2 Radio and Phone Access Privileges

Subscriber participation in Private Phone Calls is controlled by configurable checkboxes for “Private Phone Call Init” and “Private Phone Call Receive” on the radio’s SUID record in the Connect Plus user database. Whether or not a phone user can initiate or join a Group Call is controlled by the “Allow Phone Access” checkbox on the Group (and/or Multigroup) record in the user database. For connections to a SIP to PSTN device, phone user access to the system is controlled by PIN number configuration in the XRI (if “Require PIN” is enabled in the XRI). “Require PIN” is not supported (and should not be enabled) when connected to a SIP Digital Telephony Gateway. Instead, the SIP Gateway device can be used to manage phone user access.

If the SIP Gateway Device or the telephone network require the radio user to enter any special digits, this can be accomplished by sending the digits as part of the initial dial string, followed by one or more pauses (if necessary), followed by the phone number.

The radio user can request call termination by transmitting a DTMF tone, or sequence of DTMF tones (depending on XRI configuration). This is one of two methods that the radio user can use to request Private Phone Call termination in Connect Plus. For more information, see the section called, “Ending a Phone Call”.

2.20.3 Phone Calls and Resource Availability

Radio-initiated Private Phone calls require the immediate availability of both a repeater resource and an available telephone line. If a repeater timeslot is not immediately available, the radio sounds a denial tone and displays, “Phone Call Failed” (or other error message). The request is not placed in the Busy Queue. The radio user may try again at a later time. If a repeater resource is available, but a phone resource is not available, the radio sounds a negative indication tone and displays, “Phone Call Failed” (or other error message) after transmitting the initial dial string on the traffic channel.

For calls initiated by a phone user, the operation depends on the call type; Group or Private Phone Call:

[29] If the XRI will be used with a SIP Digital Telephony Gateway, the XRI must be enabled for either the Connect Plus SIP-10 or the Connect Plus SIP-20 Telephony feature prior to uploading the Key Manager File. If the XRI will be connecting to a SIP to PSTN device, then no feature license is required, but the SIP Gateway Type and IP Addresses must be defined in the uploaded Key Manager File (beginning with Release 2.6).

Phone user-initiated Private Phone calls require the immediate availability of a repeater resource, and the target radio must be available. In other words, the radio must be registered to the system, and cannot be currently involved in a call on any of its registered IDs. If either of these requirements is not met, the call does not go through, and the request is not placed in the Busy Queue. The phone user may try again at a later time.

Phone user-initiated Group Call requires immediate availability of a repeater resource at one or more the Group's registered sites. If a repeater is immediately available at one or more sites, the call is placed on the air. At other sites where a repeater isn't immediately available, the call is placed in the Busy Queue. However, if there is no repeater resource immediately available at any of the Group's registered sites, the call is removed from the Busy Queue, and the call will not go through.

2.20.4 Phone Call Initiation

The Phone Call initiation process varies according to which party is initiating the call (radio user or phone user), and what type of call is being initiated (Group Call or Private Phone Call). When the call is initiated by a phone user, the operation is different for a connection to a SIP to PSTN device and a connection to a SIP Digital Telephony Gateway.

2.20.4.1 Group Phone Call

Only the telephone user can initiate phone participation in a Group Call.

Phone User initiates call through the SIP to PSTN device: To initiate (or join) a Group Call, the phone user dials the telephone number designated for system access. When the system answers the call, it plays a voice prompt to greet the caller. If PIN Access is enabled, the user is prompted to enter a 4-digit PIN. If PIN Access is not enabled (or if the user successfully enters the PIN), the caller is prompted to enter digits to indicate the call type (Enter "1" for Group Call) and the target Group ID. If all of the information entered is valid, the system attempts to secure a repeater resource (or resources) to call the target Group. If the Group is idle, the system attempts to start a new call to the Group. If a call is already in progress for the target Group, the system attempts to join the user to the ongoing call. If the call cannot go through, the system plays a voice prompt to notify the caller. If the system is able to set-up the call, the caller hears a "join" tone when joined to the Group Call. See the section called "During a Group Phone Call" for more information.

Phone User initiates call through the SIP Digital Telephony Gateway (CUCM): When a phone user makes a call to a Group, the phone user is not prompted by the XRI to enter the Call Type and Destination ID. Instead, the SIP Gateway forwards a string of digits representing the Call Type (1 for Group Call) and the Destination ID. The phone user typically enters the string from the keypad as part of call set-up, before the string is forwarded to the XRI. The string is sometimes preceded by other digits that are required by the SIP Gateway but not conveyed to the XRI. If all of the information entered is valid, the system attempts to secure a repeater resource (or resources) to call the target Group. If the Group is idle, the system attempts to start a new call to the Group. If a call is already in progress for the target Group, the system attempts to join the user to the ongoing call. If the call cannot go through, the system plays a fast busy tone to notify the caller. If the system is able to set-up the call, the caller hears a "join" tone when joined to the Group Call. See the section called "During a Group Phone Call" for more information.

The following information is applicable to both the SIP to PSTN device and the SIP Digital Telephony Gateway interfaces:

A phone user can initiate (or join) a Multigroup Call in the same fashion as other Group Calls. When the phone user enters the Target Group ID, the system determines whether it is a regular Group Call or a Multigroup Call, depending on how the Target ID is configured in the system's user database. The phone user is not notified

whether he/she is starting (or joining) a regular group or a Multigroup. However, it is helpful for the phone user to know which ID's are used for normal groups and which ID's are used for Multigroups. If starting or joining a Multigroup Call, the phone user should not expect a radio user to talk back (unless the radio user initiated the Multigroup Call). For this reason, Multigroup IDs are best used for one-way announcements, where talkback isn't expected or required.

A phone user can join a call on a Talk Group ID that is currently being used for an Emergency Call. This is done in the same way that the phone user joins other Group Calls. It is also possible for a radio user to convert a Group Call that was initiated by a phone user to an Emergency Call. In either case, there is no special indication provided to the phone user that the call is in Emergency mode. As a general rule, the call operates the same as non-emergency calls from the perspective of the phone user. One exception is that the Call Hang Time may be extended, depending on system programming.

At the current time, a phone user is not able to initiate or join a Site All Call or Network Wide All Call.

2.20.4.2 Private Phone Call Initiated by Radio User

The radio user initiates a Private Phone call as follows:
Manual Dial – Press the Manual Phone Dial button or menu option, and then enter the phone number from the radio keypad manually. The entered digits and/or symbols are shown on the radio display. The radio user presses OK to initiate the Private Phone Call and to send the initial string.

The digits and/or symbols that are shown on the display when the radio user presses "OK" to initiate the phone call are called the "initial dial string". The initial dial string can contain up to 22 digits or symbols. The method for inserting a pause between digits (represented by the letter "P" on the radio display) depends on the radio model. For more information, please see the MOTOTRBO Connect Plus User Guide for the specific radio model of interest.

After the radio user initiates the Private Phone Call, the controller checks for an available repeater resource. If a repeater timeslot is available, the radio is assigned to a traffic channel, where it transmits the initial dial string to the controller. The radio displays "Calling" while sending the initial dial string. The radio user does not hear DTMF while entering or sending the initial dial string.

If the call attempt fails, the radio shows an error message. If the call attempt goes through, the first audio that the radio user hears after sending the initial dial string is ringing, a busy tone, or a voice message or tone from the phone line. If the phone line answers, and if there is an Interactive Voice Response (IVR) device at the phone user's end, then over dial may be required. If so, the radio user enters the over dial digits and/or symbols as described in the sub-section called, "During a Private Phone Call".

2.20.4.3 Private Phone Call Initiated by Phone User

Phone User initiates call through the SIP to PSTN device: To initiate a Private Phone Call to an individual Connect Plus radio, the phone user dials the telephone number designated for system access. When the system answers the call, it plays a voice prompt to greet the caller. If PIN Access is enabled, the user is prompted to enter a 4-digit PIN. If PIN Access is not enabled (or if the user successfully enters the PIN), the caller is prompted to enter digits to indicate the call type (Enter "2" for Private Phone Call) and the target SUID. If all of the information entered is valid, the system attempts to locate the target radio and to secure a repeater resource. If the call cannot go through, the system plays a voice prompt to notify the caller. If the system is able to set-up the call, the phone user hears ringing as the system attempts to contact the target radio. When the radio user presses PTT to answer the call, the phone user hears audio from the radio. If the radio user does not answer the call prior to the expiration of the Private Phone Call Response TOT, the system terminates the call.

Phone User initiates call through the SIP Digital Telephony Gateway (CUCM): When a phone user makes a call to a radio, the phone user is not prompted by the XRI to enter the Call Type and Destination ID. Instead, the SIP Gateway forwards a string of digits representing the Call Type (2 for Private Phone Call) and the Destination ID. The phone user typically enters the string from the keypad as part of call set-up, before the string is forwarded to the XRI. The string is sometimes preceded by other digits that are required by the SIP Gateway but not conveyed to the XRI. If all of the information entered is valid, the system attempts to locate the target radio and to secure a repeater resource. If the call cannot go through, the system plays a fast busy tone to notify the caller. If the system is able to set-up the call, the phone user hears ringing as the system attempts to contact the target radio. When the radio user presses PTT to answer the call, the phone user hears audio from the radio. If the radio user does not answer the call prior to the expiration of the Private Phone Call Response TOT the system terminates the call.

2.20.5 During a Phone Call

2.20.5.1 During a Group Phone Call

From the radio user’s point of view, a Group Call that is joined by a phone user operates very much like other group calls. Transmissions from the telephone user can be distinguished from transmissions by other radios by the Source ID of the transmission. Transmissions by a phone user are identified with a special ID code of 16776414. Just like other regular Group Calls, any participant can transmit during Call Hang Time. Also like other Group Calls, the call is terminated if no participant transmits and the Call Hang Time expires. If the Phone user initiates a Multigroup Call, the radio user is not allowed to talk back during Call Hang Time. This is the same operation as a Multigroup Call initiated by a different radio.

For the telephone user, there are several important things to know about joining a Group Call:

1. The system plays a “join tone” to notify the phone user that he/she has been joined to a Group Call.
    a. If the phone user hears voice audio after the join tone, then he/she has been joined to a call-in-progress. The phone user must wait until the radio user finishes speaking.
    b. If the phone user does not hear voice audio after the join tone, then he/she has been joined to a new Group Call. The phone user should begin speaking as soon as possible in order to continue the call. The phone user’s voice audio will be heard by any radio that has joined the call. Note: If “Manual PTT” is enabled in the XRI, the phone user must press a digit or symbol on the phone keypad prior to speaking. See item #4 for more information.
2. Only one call participant can speak at time. If the phone user speaks while he/she hears incoming audio from a radio, the phone user will not be heard by the radio(s).
3. When one participant finishes speaking, there is a limited time for someone else to talk back. This is called the Call Hang Time, and its duration depends on system configuration. If nobody speaks back during Call Hang Time, the call is terminated. Note: If the radio network supports phone user participation in Group Calls, it is recommended to set the Group Call Hang to a value that provides adequate opportunity for the phone user to talk back. The Group Call Hang Time can be set to a maximum of seven seconds via Network Manager configuration.
4. When the phone user wishes to speak to other call participants, he/she should know whether the system has been configured for VOX PTT or Manual PTT.
    a. If configured for VOX PTT, the phone user just needs to speak (when the radio user isn’t speaking). The system will detect the presence of the phone user’s voice, and begin a

transmission to the radio. In VOX operation, the phone user should avoid fluctuations in the volume of his/her voice, and the phone user should avoid pauses between words or sentences. Either of these events can make the XRI think that the phone user's transmission is finished. If so, the XRI will de-key the phone user, and the call will enter Call Hang Time.

   b. If configured for Manual PTT, the phone user presses and releases a digit or symbol on the phone keypad to key-up when he/she is ready to speak, and then presses and releases a digit or symbol on the keypad to de-key when he/she is finished speaking. The digits or symbols that are used for the key and de-key functions are configurable in the XRI. This information must be communicated to the phone user.

5. If the XRI is configured for "Manual" key-up mode, when the phone user keys the XRI, the XRI plays the key-up tone to the phone user. When the phone user de-keys the XRI, the XRI plays the de-key tone to the phone user.

6. Regardless of the method used to key into the system (VOX PTT or Manual PTT), the telephone user cannot speak indefinitely. There is a configurable XRI timer (Maximum Key Timer), which determines how long the phone user can speak for a single transmission. This important information should be communicated to the telephone user. If the timer expires, the system will automatically de-key the phone user.

7. When connected to a SIP to PSTN device, the system also supports Direct Inward Dial (DID). This feature allows the System Administrator to configure the SIP Gateway and the XRI Interconnect Gateway to skip the voice prompt and to automatically steer the phone call to a specified Talk Group ID.

2.20.5.2 During a Private Phone Call

Previous sections describe how the radio user or phone user initiates a Private Phone Call. Once the Private Phone Call is underway, it operates differently from a Group Phone Call.

Audio from the phone line is sent continuously to the radio on the repeater downlink. Because of this, the phone user does not have to do anything special to key the repeater. All he/she has to do is speak. However, this does not mean the radio user will hear everything the phone user says. The radio user can only hear the phone user while the radio is in receive mode. Therefore, the phone user should refrain from speaking while hearing incoming audio from the radio. When the radio user finishes speaking, the phone user may proceed to speak.

When the radio user wishes to speak during a Private Phone Call, he/she presses PTT and begins speaking. The radio user's audio will be passed on to the phone line regardless of whether the phone user is still speaking or not. So, the radio user doesn't have to wait for the phone user to finish speaking, but it is courteous to do so.

Another difference between Group Phone Call and Private Phone Call is that the phone user and radio user do not have be concerned with the Call Hang Time expiring. The most important timer for a Private Phone Call is the Max Call Time, which determines the maximum total duration for a Private Phone Call. It is important for both the phone user and the radio user to know the value of this system-configured timer. Starting at about ten seconds prior to expiration of the Max Call Time, the XRI plays beeps as a warning of the impending timeout. When the timer expires, the system ends the phone call.

Sometimes during a Private Phone Call in-progress, the radio user needs to send additional digits or symbols to the phone line. One example is when an Interactive Voice Response (IVR) device on the phone line prompts the radio user to enter additional digits or symbols. Any digit or symbol that is sent from the radio after the initial dial string is referred to as "over dial" or "extra digits".

The radio user can enter the over dial digits via either of the methods below:

1. “Live” over dial method.

    a. The radio user sends the over dial digit(s) by pressing and holding and PTT, and then (while continuing to hold PTT pressed), by pressing and releasing the desired keys or symbols. As each key is pressed, the radio user hears the corresponding DTMF tone.

    b. When all digit(s) have been sent, the radio user releases PTT and then listens to the incoming audio to determine whether the over dial digits have been received and processed as expected. If the over dial digits are not received and processed as expected, the radio user can repeat the process and send the digit(s) again.

2. “Buffered” over dial method. This method should only be used when the XRI is connected to a SIP to PSTN device.

    a. The radio user presses and releases the desired keys or symbols, but does not press PTT while doing so. As each key is pressed, the digit or symbol is shown on the radio display. In some models, these are called “Extra Digits”. The radio user does not hear DTMF tones when the keys are pressed.

    b. When all desired digits and/or symbols have been pressed (and are shown on the display), the radio user presses “OK”. This causes the radio to transmit the collected digits and/or symbols in a special data message to the Connect Plus controller.

    c. If the data message is decoded by the system, the digital information is converted to DTMF tones and placed on the phone line (but this might not be heard by the radio user). The radio user should listen to incoming audio to determine whether the over dial digits have been received and processed as expected. If the over dial digits are not received and processed as expected, the radio user can repeat the process and send the digit(s) again.

3. The system also supports Direct Inward Dial (DID). This feature allows the System Administrator to configure the SIP Gateway and the XRI Interconnect Gateway to skip the voice prompt and to automatically initiate a Private Phone Call to a specified target SUID.

2.20.6 Ending a Phone Call

2.20.6.1 Group Phone Call

Group Phone Call ends the same as all other Group Calls. Whenever a transmission ends, the call enters the Group Call Hang Time. If the system does not detect any further key-up to continue the call, and if the Call Hang Time expires, the call ends, and the phone user is disconnected from the Group.

At the current time, there is no way for a radio user to disconnect a phone user from a Group Call in-progress. Nor is there any means for a phone user or a radio user to terminate a Group Call prior to expiration of Group Call Hang Time.

2.20.6.2 Private Phone Call

A Private Phone Call can be terminated by one of the following actions:

1. The Private Phone Call terminates when the phone user hangs up the telephone, and the SIP Gateway device sends the XRI a message indicating call termination.

2. The Private Phone Call terminates upon expiration of Max Call Timer.

3. The Private Phone Call terminates when the site controller that set-up the call detects that the participating radio has registered with a different network site.

4. The Private Phone Call terminates if audio stream from the landline is lost or interrupted.

5. The Private Phone Call terminates if the system detects that the radio user has requested to end the phone call. There are two ways this can occur:

    a. Termination request data message

        i. If the radio user of a full-keypad, display equipped model presses the “Back” button during a Private Phone Call in-progress, the radio transmits a special data message requesting call termination. If the system decodes the message, the call is terminated. Some models require a long press of the “Back” button. For more information, please see the MOTOTRBO Connect Plus User Guide for the specific model of interest.

        ii. If the radio user of a non-display portable or numeric display mobile presses a programmable button that has been configured for the “Phone Exit” feature during a Private Phone Call in-progress, the radio transmits a special data message requesting call termination. If the system decodes the message, the call is terminated.

    b. DTMF “live” over dial termination request

        i. Whenever the radio transmits “live dial” DTMF over dial digits (see the section called “During a Private Phone Call”), the system compares the decoded DTMF digits to the “DTMF Hang up Sequence” that has been configured into the XRI. The Radio Hang Up sequence can be from 1 to 5 digits or symbols, and each digit or symbol can be configured for “short tone” or “long tone”. If the decoded digits or symbols match the configured sequence, the call is terminated.

Regardless of which method is used to request call termination (termination request data message or DTMF “live” over dial), the radio user should listen to incoming audio to determine whether the termination

attempt was received and processed as expected. If not, the call continues and the radio user can repeat the attempt again.

2.20.7 Enhanced Privacy Considerations

Group Phone Calls: If any radio transmits secure (encrypted) audio during a Group Call with a phone line participant, the audio will not be intelligible to the phone line user. For this reason, the radio user should disable the Enhanced Privacy transmit function when a Group Call has a phone line participant. The radio user knows that a phone user has started or joined the Group Call when he/she sees a transmission identified with the special ID code of 16776414.

Private Phone Calls: The radio automatically disables the Enhanced Privacy transmit function during a Private Phone Call. If the Enhanced Privacy transmit function was enabled prior to initiating or receiving the Private Phone Call, the radio will automatically re-enable the function when the Private Phone Call is over.

2.20.8 Phone Line Considerations

When connected to a SIP to PSTN device, Connect Plus Telephone interconnect supports connection of a maximum of sixteen PSTN, POTS, or PBX phone lines (depending on the capability of the SIP Telephone Gateway device). When connected to a SIP Digital Telephony Gateway, Connect Plus Telephone Interconnect supports either 10 or 20 simultaneous phone calls, depending on the feature license in the XRI Interconnect Gateway.

When connected to a SIP to PSTN device, Connect Plus does not currently steer a radio-initiated Private Phone Call to a specific phone line, based on the number dialed or any other consideration. Any available line will be used. For this reason, all attached phone lines must be able to handle the same radio-supplied dial string in the same way. The practical application of this operation is as follows:

1. If any of the attached phone lines is attached to the public phone network, then all phone lines configured in the XRI must be attached to the same LATA (Local Access and Transport Area) in the same public phone network.

2. If any of the attached phone lines is attached to a PBX or private phone network, then all phone lines configured in the XRI must be attached to the same PBX or private phone network.

When connected to a SIP Digital Telephony Gateway, all radio-initiated Private Phone Calls are sent to the connected SIP Gateway device. The SIP Gateway device examines the dial string and determines where the call should be routed based on the configuration of the SIP Gateway device.

2.20.9 Phone Logs, Call Logs and Event Logs

The XRI provides a downloadable phone call log. Some of the items captured on a per call basis are as follows: type of phone call, SIP Gateway Resource (phone line) used when connected to a SIP to PSTN device, call duration, call start time, Group ID or Radio ID participating in the call, and number dialed (radio-initiated calls only).

The XRC Controller provides a downloadable ATR (airtime record) log, which records phone calls from the repeater airtime perspective. The airtime record includes the following information on a per-call basis:

- Group Call: Source ID, Destination Group ID, Repeater and slot, call duration and key record. The Phone user is identified with the special code of 16776414.

- Private Phone Call: Source ID, Destination ID, Repeater and slot, and call duration. The Phone user is identified with the special code of 16776414.

The XRI has a downloadable Event Log to capture errors and events of interest to the System Administrator. When the Event Log archive exceeds a size of 100 MB, the oldest entries are automatically purged.

2.20.10 Phone Call Supervision (voice prompts)

When connected to a SIP to PSTN device, Connect Plus Telephone Interconnect utilizes voice prompts to provide supervision (guidance) to the phone user during call set-up and to notify the phone caller of some events during established calls, such as call termination.

When connected to a SIP Digital Telephony Gateway, Connect Plus Telephone Interconnect does not utilize voice prompts during call set-up, but does utilize some voice prompts at call termination.

By default, the XRI provides a set of English-language voice prompts.

In addition, the XRI (via the Network manager) provides the ability to upload customer-supplied prompts as substitutes for the default prompts. If desired, the customer can replace the default English prompts with customer-supplied prompts in another language. There are a number software programs available that allow the user to record audio and to specify the digital audio file characteristics. Customer-supplied prompts must meet the following criteria.

- The audio file must contain 16 bit, uncompressed, PCM digital audio.
- The audio file must NOT contain any file header.
- The audio file byte order must be little endian.
- The digital audio sample rate must be 8 kHz.

2.20.11 SIP Digest Authentication

SIP Digest Authentication is supported for connection to a SIP Digital Telephony Gateway only.

When SIP Digest Authentication is enabled, the XRI Interconnect Gateway and the connected SIP Digital Telephony Gateway check whether they have been configured with matching SIP Digest settings (also called “credentials”). Telephone calls are not allowed unless the devices confirm a match.

If SIP Digest Authentication is enabled in the XRI, then it must also be enabled in the SIP Digital Telephony Gateway (and vice versa), and both devices must be configured with the same SIP Digest character strings. The

setting names may be somewhat different in the XRI and in the SIP Gateway, and the SIP Digest settings may have to be configured into more than one location in the SIP Gateway device configuration software.

2.20.12 IP Address Considerations

The following devices require a Static IP address for Connect Plus Telephone Interconnect operation.

- XRI interconnect Gateway
- Each SIP Gateway device. Beginning with MOTOTRBO Release 1.7 (R2.6.0), the SIP Gateway IP Addresses that will be used by the XRI must be encoded in a special Key Manager File and uploaded to the XRI. For more information, see section "Key Manager File and Feature License."
- Each XRC Controller
- Each XRT Gateway

2.20.13 Telephone Interconnect System Configuration

This section provides a brief configuration overview for the various Connect Plus Telephone Interconnect components. It also tells where to find additional information for each device.

2.20.13.1 SIP Gateway Device Configuration

The configurable settings of the SIP Gateway Device will vary according to the manufacturer, model, and available features.

As an example, some of the most important settings for the Cisco SPA8800 are as follows. These settings are configured for each Line tab (1-4) that is used for the SPA8800. The settings below may not be available for all SIP Gateways, or the setting names may be different.

- SIP Transport: UDP
- SIP Port: The UDP port desired by the system infrastructure owner to allow inbound communication to each phone line. This port number is required to be unique for each line. The value configured for this field is also entered into the "UDP Port" field on the XRI's SIP Gateway Configuration screen (for the entry corresponding to this line).
- Proxy: IP Address of the XRI
- Outbound Proxy: IP Address of the XRI
- Use Outbound Proxy: Yes (Allows the SPA8800 to send SIP requests to the XRI for inbound calls.)
- Register: No (The SPA8800 is not required to register with the SIP proxy for use with the XRI.)
- Make Call Without Registration: Yes (Allows the SPA8800 to dial calls upon request by the XRI.)
- Answer Call Without Registration: Yes (Allows the SPA8800 to answer inbound calls destined for the XRI.)
- Preferred Codec: G711u (This is the 8 Bit PCMu codec required by the XRI).
- Dial Plan: (P0:0)

A SIP Digital Telephony Gateway, such as the Cisco Unified Communications Manager (CUCM), requires somewhat a complex configuration, which is beyond the scope of this document, and should be performed by seasoned IT personnel; preferably a person certified in Cisco telephony technologies. A few of the most important settings configured with the **Cisco Unified CM Administration** interface are as follows:

- The XRI Interconnect Gateway is a configured as a Device Trunk in the CUCM. Device Trunk settings include:

  - Device Name for the XRI. This is used to distinguish from other Trunks and to link the trunk configuration to other CUCM configuration screens.
  - Device Pool. The Device Pool is configured on a separate screen.
  - XRI's IP address and SIP Listen Port.
  - SIP Security Profile to be used with the XRI. The SIP Security profile is configured on a separate screen. It provides the ability to enable (SIP) Digest Authentication and Application Level Authentication. When Digest Authentication is enabled, the XRI's SIP Digest Settings (Realm, User, Credentials) must be entered on the CUCM's SIP Realm Screen. When Application Level Authentication is enabled, the XRI's SIP Digest Settings (User and Credentials) must be entered on the CUCM's Application User Screen.
  - SIP Profile to be used with the XRI. The SIP Profile is configured on a separate screen. The SIP Profile Screen can be used to enable the "SIP Options Ping", which allows the CUCM to monitor and display the status of its IP connection to the XRI, even when there is no call activity.

- Another important configuration step is to configure the Route Pattern screen. The Route Pattern determines which dial strings entered by phone users will be forwarded to the trunk indicated by the screen's Gateway/Route List setting. The Route Pattern screen also defines which digits should be discarded prior to forwarding the dial string to the XRI. The first digit forwarded to the XRI must represent the Call Type ("1" for Group Call, "2" for Private Phone Call) while the remaining forwarded digits represent the Destination ID.
- The Cisco Unified CM Administration interface is also used to configure the phones and other resources controlled by the CUCM.

Note: The above discussion of CUCM settings is not all-inclusive.

For a complete list of configurable settings in the SIP Gateway Device, please consult the manufacturer's official product documentation.

2.20.13.2 Connecting to the XRI

The MOTOTRBO Connect Plus Network Manager Connection Tool is used for connecting to the XRI Interconnect Gateway, in much the same way as it used to connect to XRC Controller Sites. When creating the connection, the Network Manager Connection Tool user must select "XRI" as the Device Type.

XRI connections can be included in a Group connection along with XRC Controller sites. As with any Group connection, all devices in the Group (including the XRI) must accept the Username and Password that is entered when initiating the Group connection. The Site Dashboard shows the status of the connection to the XRI and the status of the connection(s) to any controller site(s) included in the Group.

For more information on connecting to an XRI, see the XRI Interconnect Gateway User Guide or the MOTOTRBO Connect Plus Network Manager Help file.

2.20.13.3 XRI Configuration

The MOTOTRBO Connect Plus Network Manager is used to configure the following information for the XRI Interconnect Gateway:

- XRI IP address information
- SIP UDP Listen Port: In most cases, this should remain set to the default value of 5060, the “well-known” port for SIP connections.
- IP address and port information for XRC Controller sites and XRT Gateway sites
- IP address and port information for SIP Gateway resources
- Enable and configure SIP Digest Authentication (optional). This feature is only applicable for connections to a SIP Digital Telephony Gateway.
- Configurable phone call timers
- Selecting the phone user key-up method for Group Calls
- Enabling & configuring call termination via DTMF (optional)
- Enabling PIN access for phone users & configuring PINs (optional). This feature is only applicable for connections to a SIP to PSTN device.

The Network Manager also provides the ability to monitor the status of IP connections between the XRI and other devices, to set the XRI time and date, to configure XRI User Roles, and to overwrite the default English voice prompts with customer-supplied prompts (optional).

For more information on XRI Configuration, see the XRI Interconnect Gateway User Guide or the MOTOTRBO Connect Plus Network Manager Help file.

2.20.13.4 XRC Controller Configuration

The MOTOTRBO Connect Plus Network Manager is used to configure several XRC Controller settings that impact Connect Plus Telephone Interconnect operation:

- XRI TCP Listen Port
- Private Phone Call Response TOT: Determines how long the XRC attempts to contact (ring) the target radio at the beginning of an inbound Private Phone Call.

- User Registry Settings
  - Allow Phone Access: Configurable per Group and Multigroup Record
  - Private Phone Call Initiation privilege: Configurable per SU record
  - Private Phone Call Receive privilege: Configurable per SU record

For more information on XRC Controller Configuration, see the XRC Controller User Guide or the MOTOTRBO Connect Plus Network Manager Help file.

2.20.13.5 XRT Gateway Configuration

The MOTOTRBO Connect Plus XRT Configuration Tool is used to configure the XRT Gateway. At the current time, the XRT Gateway Client can participate in Group Calls that include a phone user, but cannot initiate or receive Private Phone Calls. Configurable XRT settings that impact phone call operation include:

- XRI TCP Listen Port
- Allow Phone Access: User Registry setting that is configurable per Group and Multigroup Record.

In order to participate in a Group Call that has a phone user as participant, the XRT Client must register the Group Talkpath ID used for the call (prior to the start of the call), and the “Allow Phone Access” box must be checked on the Group (or Multigroup) record in the Connect Plus user database. Transmissions by a phone user are identified with a special ID code of 16776414.

For more information on XRT Gateway Configuration, see the XRT Gateway User Guide or the MOTOTRBO Connect Plus XRT Configuration Tool Help file.

2.20.13.6 Repeater Configuration

There is no special repeater configuration required for Connect Plus Telephone Interconnect operation (beyond the normal Connect Plus repeater configuration). It should be noted that the controller will assign phone calls to any available repeater. Therefore, the Time Out Timer (TOT) in all repeaters must not be shorter than the Max Call Time in the XRI.

The Telephone Interconnect feature does not need to show as “Purchased” (enabled) on the MOTOTRBO CPS Device Information screen. That feature applies to non-Connect Plus modes of operation only.

2.20.13.7 Radio Configuration

Configuring the radio with MOTOTRBO CPS

There is no special MOTOTRBO CPS radio configuration required for Connect Plus Telephone Interconnect (beyond the normal MOTOTRBO CPS radio configuration for Connect Plus operation).

It should be noted that the box labeled “Private Calls” on the MOTOTRBO CPS General Settings screen must be checked for the radio to participate in both Private Calls and Private Phone Calls. This is because Connect Plus utilizes Private Call signaling to pass audio during Private Phone Calls.

Configuring the radio with MOTOTRBO Connect Plus CPS

Connect Plus CPS configurable phone parameters vary by radio model.

1. Private Phone Call initiation
    a. For a full-keypad, display equipped model to initiate a telephone call, it must have a means of entering or selecting the target phone number.
        i. The box labeled “Phone Manual Dial” should be checked on the Connect Plus CPS Menu screen. This allows the radio user to access the Phone Number entry screen.
        ii. If desired, the radio can be configured for a “Phone Manual Dial” programmable button, which acts as a shortcut to the Phone Number entry screen.
2. Private Phone Call Termination. Radios that participate in Private Phone calls should have a means for requesting the system to end the Phone Call.
    a. For full keypad, display-equipped radios, there is no special configuration required. The radio user can request to end the Private Phone Call by pressing the “Back” button during a phone call in-progress. Some models require a long press of the “Back” button. For more information, please see the MOTOTRBO Connect Plus User Guide for the specific model of interest.
    b. Non-display portable radios and numeric display mobiles must be configured with the “Phone Exit” programmable button in order to request the system to end a Private Phone Call.

For more information on Connect Plus radio configuration, please see the MOTOTRBO Connect Plus CPS Help File.

For more information on Connect Plus radio operation, please see the MOTOTRBO Connect Plus user guide for the radio model of interest.

3 Connect Plus System Components and Topologies

3.1 Connect Plus System Components

The System Components of a Connect Plus System are similar to those of other digital modes, such as IP Site Connect or Capacity Plus. The reader can refer to the section on *System Components* of [1] for detailed information on the MOTOTRBO equipment and specifications. The primary differences for Connect Plus System Components are listed immediately below. These differences will be discussed in greater detail in the sections that follow:

System Components of Connect Plus that are not used in other MOTOTRBO digital modes:

- XRC controller

System Components used in other digital modes that are not used in Connect Plus:

- Radio Control Station as the LRRP and Text Message application interface
- Text Message terminal connected directly to SU via USB
- Multi-Channel Device Driver (MCDD)

3.1.1 Fixed End Components

3.1.1.1 XRC Controller

Each Connect Plus site requires at least one XRC Controller. If desired, the customer may purchase a second XRC Controller per site to serve as backup to the primary XRC. The secondary XRC can be configured to assume site control if the primary XRC fails, provided that the secondary controller has IP connectivity with its local repeaters. The secondary controller provides backup capability, but it does not increase the number of repeaters and calls that can be managed per site.

The XRC controls up to 15 MOTOTRBO repeaters per trunked site. Because this is an IP interface, the XRC and its connected repeaters could theoretically be in different locations. However, due to the time sensitive nature of the messaging between the controller and the repeaters, the XRC and its trunked repeaters must be at the same physical location and connected to the same Ethernet switch. Other configurations are neither recommended nor supported.

Because the repeaters operate in digital mode, the XRC can control up to 30 digital channels (timeslots) per Connect Plus site. One of these timeslots must be dedicated for Control Channel signaling. All other timeslots are used by the controller for call assignment. Any timeslot that is not the Control Channel timeslot is a “trunk-to” timeslot. This term is used because the SU moves or “trunks” to the slot after receiving a call assignment message on the Control Channel downlink.

The XRC communicates with its trunked repeaters via the Link Establishment (LE) Protocol. The XRC is configured as the LE Master and requires a static IP address. Its repeaters are configured as LE Peers. Repeater IP addresses may be static or assigned via DHCP.

XRC Functions for its Local Site

The XRC acts as the site controller for its co-located repeaters. It communicates with the repeaters via IP in order to:

- Act as Link Establishment (LE) Master
- Encode & Decode Control Channel messaging
- Process registrations and Call Requests
- Track which RF resources are (and are not) currently available
- Assign RF resources
- Maintain a Busy Queue when no RF resources are available
- Repeat transmitted audio packets on the repeater downlink
- Receive text messages created by SU's that are registered to the site.
- Deliver text messages addressed to SU's that are registered to the site.
- Receive Location Requests sent by the Location Server or forwarded from other sites.
- Deliver Location Requests addressed to SU's that are registered to the site.
- Receive Location Reports from SU's that are registered to the site, and forward the reports to the Location server.
- Assist repeater with FCC compliance (CWID, Level I and II Monitoring)
- Track airtime usage other site statistics

XRC Multisite Functions

The ability to operate in a multisite network is a purchasable option for the XRC controller. If multisite networking is desired, each Connect Plus site requires an XRC controller, and each XRC must be enabled for multisite operation.

Each XRC only has direct control over the MOTOTRBO repeaters at its own site location. In multisite operation, the XRC controllers communicate with one another via IP to facilitate multi-site call set-up and audio routing. TCP/IP is used for call set-up messages. Audio packets are transported via UDP/IP.

In a multisite network, the controller has all of the same responsibilities that it has in single site mode, along with several additional functions as listed below:

- Track registrations and de-registrations throughout the Connect Plus network
- Based on its list of registered SU's and Groups, efficiently assign local RF resources for inbound network calls.
- Facilitate network call set-up
- Duplicate and forward voice packets to any site where the Target ID is registered
- Provide voice arbitration in the event of simultaneous or near-simultaneous voice transmissions at multiple Connect Plus sites. When the XRC receives voice packets from multiple sources for the same call, the controller uses time stamps to decide which voice stream will be transmitted on the repeater downlink under its control.
- When receiving a Text Message or Location Request for a registered SU from another site, or from a third party application, the XRC transmits the message or request to the registered SU.
- When receiving a Text Message or Location Request for an SU that is registered to a different network site, the XRC routes the message to the site where the Target ID is registered.
- Send a periodic "Neighbor Site" message to tell SU's which network site(s) is/are RF-adjacent to this one.
- Provide NTP service to the other site controllers if configured through the Network Manager. For more information on the NTP settings the reader can refer to [4].

User Database

Each XRC Trunking Controller and XRT Controller Gateway maintains a copy of the Connect Plus user database, also called the User Registry. The user database contains a list of user records (both subscriber unit records and talkgroup records) that are used to validate radio registrations and call privileges.

In some trunked radio systems the user database is kept by a single piece of hardware at a single location, which makes the system susceptible to a single point of failure. In Connect Plus, however, all controllers strive to maintain an identical copy of the user database. If a change is made to any user record at any XRC or XRT, the change is automatically propagated to all network sites. This architecture allows registrations and call requests to be validated, even when the validating site is experiencing temporary connectivity problems to other parts of the Connect Plus network. However, it is important to emphasize that good connectivity is essential to satisfactory network operation. Dependable connectivity helps assure that a radio will hear all of its intended calls, no matter where it is located in the network.

While the Connect Plus architecture allows user records to be edited after connecting to any Connect Plus site, it is strongly recommended that the Network Administrator designate one network site as the preferred site for making changes to the user database. This information should be communicated to all persons who will be adding and/or editing user records. When the user record is edited at the preferred site, the Connect Plus network will automatically propagate the change to other sites. Establishing this policy helps assure that one site has a reliable "master" copy of the user database that can be copied to other sites when necessary. It also helps prevent problems that can arise if the same user record is simultaneously edited (or near-simultaneously edited) at multiple Connect Plus sites.

Even though the Connect Plus software strives to maintain an identical copy of the user database at all network sites, network connectivity issues can potentially cause the database to vary from one site to another. If such a variance should occur, it may show up as a difference in operation (such as a successful registration or call request at one network site, but an invalid registration or call request at another site in the same network). In most cases, these variances will automatically correct themselves within a few minutes of re-establishing connectivity.

However, if the problem persists, the Network Administrator may need to take some corrective action to re-synchronize the user database at all sites.

The MOTOTRBO Connect Plus Network Manager (the software tool used to configure the XRC Controllers) provides the “User Health” feature. This screen allows an authorized technician to quickly determine whether all sites have the same copy of the user database. If not, the feature provides the ability to efficiently copy the database from a known “good site” (the preferred site for making database changes) to other network sites. In most cases the software does not need to copy the entire database. Instead, the software automatically identifies which section of the database is out of sync, and copies only that section. For more information on this feature, refer to the MOTOTRBO Connect Plus XRC Controller User Guide.

The XRC Controllers and XRT Gateways in the same Connect Plus network have the ability to automatically detect differences in their copies of the Connect Plus user database, and to automatically synchronize their database records with other XRC/XRT devices. The process occurs behind the scenes without user intervention (assuming good network connectivity and sufficient time to detect and resolve database differences). The devices synchronize their user records based on the most recent timestamp. Therefore, it is very important to synchronize all XRC/XRT clocks to the same Network Time Protocol (NTP) Server. For more information, see the XRT Controller and/or XRT Gateway User Guides.

Until the databases are completely synchronized, the Network Manager user may still notice differences between the “UR Fingerprints” of different network sites (as observed with the Network Manager’s User Health Tool). In most cases, the databases (and the corresponding “UR Fingerprints”) will synchronize automatically, and it will not be necessary to use the Network Manager User Health Tool to push the user database from one device to another.

XRC Configuration & Programming

The XRC controller must be configured for proper operation. This configuration can be accomplished either locally or remotely by using the MOTOTRBO Connect Plus Network Manager software. The Network Manager is used to:

- Validate and configure privileges for Connect Plus subscribers
- Configure site and network parameters
- Monitor site RF activity in real time
- Monitor airtime usage and diagnostic information
- Perform XRC controller storage maintenance, namely clearing old airtime logs

For more information on the MOTOTRBO Connect Plus Network Manager, see the section “Other IP Components of the Connect Plus Multisite Network”.

3.1.1.2 Repeater Operation in Connect Plus

The MOTOTRBO repeater interfaces with the XRC Controller to provide the RF interface for the Connect Plus site. Each XRC can control up to 15 MOTOTRBO repeaters, for a total of 30 digital channels (timeslots).

The repeater must be enabled for digital operation and configured as a Peer in the Link Establishment settings on the MOTOTRBO CPS Network screen. The XRC serves as the Master. For a more thorough discussion on

MOTOTRBO CPS programming requirements for the MOTOTRBO repeater, see “Connect Plus System Design Considerations”.

The repeater must be enabled for Connect Plus operation via MOTOTRBO CPS configuration. As a Connect Plus repeater, its operation differs from other digital modes in several ways:

- In Connect Plus operation, the repeater doesn’t automatically repeat everything it receives on its uplink. Instead, it forwards received transmissions to the XRC controller. The controller decides whether to route the transmission back to the repeater downlink.

- The Connect Plus controller only routes “authorized transmissions” back to the repeater downlink. An authorized transmission is one that has been initiated and validated via Connect Plus messaging on the Control Channel timeslot. Because of this, a conventional (non-Connect Plus) SU cannot utilize the repeater as long as the downlink is under Connect Plus control. If a conventional SU (operating in digital mode) attempts to initiate a call on a Connect Plus repeater, its transmission will be received by the repeater and forwarded to the controller, but the controller will not repeat the transmission on the downlink. This feature prevents unauthorized “pirating” of Connect Plus channels. However, if IP communications between the XRC controller and the repeater are disrupted for an extended period of time (at least a minute or longer), the repeater will enter “Conventional Fallback Mode”, in which it operates as a digital conventional repeater. In Conventional Fallback Mode, the repeater will automatically repeat the transmissions of a correctly programmed conventional SU. For a more thorough discussion on Connect Plus operation in the presence of failures, see the “Connect Plus System Design Considerations” section.

- In conventional IP Site Connect, a radio transmission received by one IP Site Connect repeater is not only repeated on its own downlink, it also transmitted by all other IP Site Connect repeaters – regardless of whether any SU is currently present to receive the call. In Connect Plus, each downlink timeslot is controlled independently, thereby allowing for efficient utilization of network RF resources. A Group voice call, for example, will only be heard at sites where a Group member is currently registered. If a Group member is not currently registered, the site is not brought into the call.

- In conventional IP Site Connect, IP Site Connect functionality can be enabled or disabled per repeater timeslot. The available options are “None”, “Slot 1”, “Slot 1 & 2”, or “Slot 2”. When using the repeater for Connect Plus, the XRC Controller will assume it has access to both repeater timeslots. Therefore, the Connect Plus repeater must be configured for IP Site Connect on “Slot 1 & 2” with MOTOTRBO CPS. This rule is not enforced by MOTOTRBO CPS, but it is required for proper operation.

- In other digital modes, the repeater is programmed with a Radio ID in the range of 1 to 16776415. In Connect Plus, each repeater in the Connect Plus site must be programmed with a unique Radio ID in the range of 1 to 15. Repeaters in other Connect Plus sites will use this same range (1-15). This rule is not enforced by MOTOTRBO CPS, but it is required for proper operation.

- In other digital modes, Base Station Identification (also called CWID) is handled entirely by the repeater. In Connect Plus mode, CWID is handled jointly by the repeater and the XRC controller. The CWID itself (usually the FCC license call sign) is programmed into the repeater with MOTOTRBO CPS, but the CWID TX Interval is programmed into the controller. In Connect Plus mode of operation, the repeater knows to ignore the CWID TX Interval programmed with MOTOTRBO CPS. The Controller will tell the repeater when to send CWID. For a more thorough discussion on CWID, see the “Connect Plus System Design Considerations” section.

- In other digital modes, FCC Type I compliance is handled entirely by the repeater itself, and FCC Type II compliance is handled by the repeater after being initiated by an external input. In Connect Plus mode, the repeater operates in much the same way, but it also takes the additional step of informing the XRC

controller when it has taken itself off-line. This is necessary so that the controller will not try to assign calls to the repeater until the repeater reports itself back on-line.

- In other digital modes, the repeater downlink uses embedded signaling to indicate the status of the repeater timeslots. This embedded signaling rides in more than one part of the transmitted signal. In Connect Plus, some of this embedded signaling is used just as in other digital modes, while other parts of the embedded signaling convey information that is unique to Connect Plus.

- In Connect Plus mode, the repeater acts as a "conduit" for Connect Plus control messages, but it does not process the messages. The messages are processed by the XRC controller and the Connect Plus SU.

- In Connect Plus mode, the XRC controller provides voice arbitration in the event of simultaneous or near-simultaneous voice transmissions at multiple Connect Plus sites. This differs from conventional IP Site Connect operation, where voice arbitration is done by the repeater itself.

- The Call Hang Time values programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Call Hang Time values that have been programmed with the MOTOTRBO Connect Plus Network Manager. The repeater will use the Network Manager-configured values as long as it maintains its connection to the XRC. Regardless of which method is used to set the Call Hang Times, Connect Plus requires the following:

  - In conventional operation, the repeater can be configured with a "zero" Call Hang Time to create a "transmission trunking" environment where each PTT is treated as a brand new call. This configuration is not supported in Connect Plus because the time required for Control Channel call processing, validation, channel assignment, and synchronization with the assigned timeslot would have to be repeated for each PTT. Connect Plus recommends that Call Hang Time values be set to 3 seconds (or longer) for each call type.

  - The Hang Time value selected for each call type must be programmed the same in all Connect Plus repeaters, at all sites, network-wide.

For more information on repeater configuration and operation for Connect Plus, see the "Multiple Digital Repeaters in Connect Plus Mode" section in "Connect Plus System Design Considerations".

3.1.1.3 Radio Control Station in Connect Plus

The Control Station Radio, an important system component in other digital modes, is not necessary in Connect Plus for Text Message Services and Location Services.

In other digital modes, a Text Message application or Location application resides on a PC that has a USB connection to a mobile radio, serving as Control Station. The Control Station radio acts as peer to other subscriber units in the field via the Common Air Interface. Connect Plus does not use this architecture. In Connect Plus, the Text Message or Location application resides on a PC that is connected via IP to a XRC Controller. This can be any Connect Plus controller on the radio network. The controller is the application's gateway to the Common Air Interface. This architecture provides significant advantages because the XRC Controller is the system component with the required knowledge to locate the destination SU, identify an available RF resource, and deliver the message to its intended target.

Other digital modes utilize Control Stations as the application gateway for GPS Revert or Data Revert Channels. The SU picks which "revert channel" to use based on MOTOTRBO CPS programming. This strategy is not used in Connect Plus. Instead, the XRC Controller assigns timeslots for all data calls. In doing so, the controller may use any available timeslot.

Connect Plus supports radio control via an IP based software application (also called the “IP Peripheral”). The IP Peripheral connects via a MOTOTRBO mobile radio equipped with a Connect Plus Option Board. This allows a remotely controlled mobile radio to request calls in much the same way as other subscriber units, thereby facilitating a wireless console interface (or similar applications). When the Connect Plus radio is utilized as a control station for an IP Peripheral, the features that can be initiated by a local radio user (manipulating the radio’s physical buttons) are limited to Push-to-talk (PTT) press and Emergency Initiation through a programmable button. Other features must be initiated via the IP Peripheral application.

3.1.1.4 MC1000, MC2000, MC2500 Console in Connect Plus

The MOTOTRBO Connect Plus mobile supports the MC Deskset Series of consoles. The MC Deskset Series provides a complete portfolio of products for a small control room. The portfolio ranges from a simple talk and listen unit to a miniature multi-channel console.

The MC1000, connected through its Tone Remote Adapter (TRA), can control a single control station, and provides a selection of up to four Connect Plus Channel Rocker positions. Each of these Channel Rocker positions can be used to start a Group or Private Call, depending on how the radio is programmed with MOTOTRBO Connect Plus CPS. This unit requires no software for programming.

The MC2000, connected through its TRA, can also control a single control station, but provides a selection of up to 16 Connect Plus Channel Rocker positions. Each of these Channel Rocker positions can be used to start a Group or Private Call, depending on how the radio is programmed with MOTOTRBO Connect Plus CPS. This unit is programmed by using configuration software installed on a PC.

The MC2500 controls up to 4 control stations (one TRA per Control Station). Each control station provides a selection of up to 16 Connect Plus Channel Rocker positions. Each of these Channel Rocker positions can be used to start a Group or Private Call, depending on how the radio is programmed with MOTOTRBO Connect Plus CPS. This unit is programmed by using configuration software installed on a PC.

The TRA interfaces to the control station using the 26-pin MAP connector. The console interface to the control station consists of TX_Audio, RX_Audio, and External PTT. Additionally, Talk Group steering is provided by the control station and Connect Plus Option Board through the GPIO pins, which are configurable using both MOTOTRBO CPS and MOTOTRBO Connect Plus CPS.

The Connect Plus interface does not require pins to be assigned to the Monitor or Channel Activity functions. This is because the control station always monitors a “busy” channel (the Control Channel) while idle. This will not prevent the console operator from the making a call request. Supervisory tones such as the Talk Permit Tone and the Busy Tone are provided to the console operator by the Connect Plus radio. These tones tell the console operator how the Connect Plus System is handling the radio’s call request.

3.1.1.5 XRT Gateway

The XRT Gateway is an optional component of the MOTOTRBO Connect Plus digital trunking system. The XRT Gateway is designed to perform protocol translation for equipment and applications wishing to interact with the Connect Plus system. The XRT is an Internet Protocol (IP) based device that allows connectivity from authorized clients that are part of the Motorola Solutions Application Development Partner (ADP) Program.

There are two XRT models - XRT 9000 and XRT 9100[30]. The XRT 9100 provides the same features as the XRT 9000, along with faster processing, more memory, and external heat dissipation.

The XRT Gateway Protocol Specification defines the messages that provide access to the following features:

- Group Call
- Multigroup Call
- Network Wide All Call
- Private Call
- Emergency Call
- Notification of radio-initiated Emergency Alert
- Call Alert
- Radio Monitor
- Radio Check
- Radio Enable
- Radio Disable
- Packet Data Call
- Generic Data Call

When the client application establishes communication with the XRT, messages are exchanged to identify the client, to check authorization, and to enforce client privileges as configured into the XRT. Client privileges include access to airtime logging data from the Connect Plus network and the ability to register Talk Paths with the XRT. Group Talk Paths support group communications with Connect Plus radios. Private Talk paths support individual communications, such as Private Calls, Radio Check, etc. A Data Path is a special type of Private Talk Path that allows the Client software to send and receive Raw Data Packets as discussed in section “Connect Plus Integrated Data”.

The total number of Talk Paths (including Data Paths) registered by all clients cannot exceed the number of Talk Paths licensed for the XRT, which is a maximum of 100 for XRT 9000 and 750 for XRT 9100. The number of licensed Talk Paths determines how many Group and Private IDs can be registered by all clients, but not the maximum number of simultaneous calls. The maximum number of simultaneous calls on a single XRT is 30 for XRT 9000 and 100 for XRT 9100. This total includes voice calls and non-voice calls (Call Alert, Radio Check, Enable, Disable etc). Packet Data Calls and Generic Data Calls do not count against the limit of simultaneous calls. Use the XRT Configuration Tool’s Feature Status Screen to view the number of Talk/Data Paths that are currently licensed for the XRT Gateway. This screen can also be used to increase the number of Paths that are licensed to the device.

Third party client applications are available to perform the following functions through their interface to Connect Plus via the XRT Gateway:

- Connect a digital, wireline console to the Connect Plus network
- Automatically retrieve and process airtime data from the XRC controllers
- Provide Connect Plus connectivity for certain 2-wire and/or 4-wire analog devices
    - Converting analog audio to AMBE+2™ digital audio
    - Converting AMBE+2™ digital audio to analog audio

Exchange raw data packets with a Non-IP Peripheral device connected to a Connect Plus mobile radio as discussed in the section “Connect Plus Integrated Data”. The packets are called “raw data” because the data

[30] For any diagram in the Connect Plus System Planner that depicts the XRT 9000, the device can be either a XRT 9000 or a XRT 9100. Wherever a textual statement or feature description applies to both hardware platforms, the term “XRT” is used.

payload is generated and interpreted by the two devices at either end of the connection (the XRT Client and the Non-IP Peripheral device). The Connect Plus infrastructure does not understand the meaning of the data. It merely serves as the conduit for transporting the packets.

In the future, the number of client applications that can access the Connect Plus system via the XRT, and the number of features provided by those applications, is expected to grow.

To the Connect Plus system, each XRT looks very much like another Connect Plus site. In fact, the XRT is assigned a special site number, and must be listed in the Multisite Configuration of the XRC controller(s). A single site system (i.e. a XRC controller that is not enabled for the multisite feature) supports a maximum of one RF site and one XRT Gateway. Because the XRT Gateway is configured as Site 255, the term “single site system” is somewhat of a misnomer. A Connect Plus multisite system supports a maximum of five XRT Gateways (site numbers 251-255).

The MOTOTRBO Connect Plus XRT Configuration Tool is the software application used to configure the XRT Gateway. This application can connect to the XRT via IP, or by using a serial connection.

3.1.2 Mobile Components

3.1.2.1 MOTOTRBO Portable Radio

The Connect Plus MOTOTRBO portable is available in two tiers:

- A keypad radio with display, and
- A non-keypad radio with no display

Connect Plus mode portable radio has slightly different battery life characteristics compared to the radios configured to operate in other MOTOTRBO digital modes due to the presence of the Option Board, which consumes additional power. The following table lists the average battery life at 5/5/90 duty cycle with battery saver disabled; no attached accessories, automatic roaming disabled and transmitting at high power. Actual performance may vary by band and usage characteristics. The high-capacity battery (2150 mAh) is recommended for use with Connect Plus portables.

Battery Type	Average Battery Life (voice only)	Average Battery Life (GPS on)
IMPRES Li-Ion 2150 mAh	14.5 Hours	13.0 Hours
IMPRES Li-Ion 1400 mAh (FM)	9.5 Hours	8.0 Hours
IMPRES Li-Ion 1750 mAh[31]	11.5 Hours	10.0 Hours

Table 3-1 Expected Battery Life

For more details on the MOTOTRBO Portable Radio the reader can refer to the *MOTOTRBO Portable* section in [1].

[31] For use with portables certified as *intrinsically safe* by CSA (Canadian Standards Association).

3.1.2.2 Portable Radio Accessories & Peripherals Interface

The configurable pin options provided by MOTOTRBO CPS for the portable radio are not presently supported in Connect Plus. They currently apply to non-Connect Plus modes only.

3.1.2.3 MOTOTRBO Mobile Radio

The Connect Plus MOTOTRBO mobile is available in two tiers:

- A radio with full display, and
- A radio with numeric display

For more details on the MOTOTRBO Mobile Radio the reader can refer to the *MOTOTRBO Mobile* section in [1].

3.1.2.4 Mobile Radio Front Panel Accessory Interface

For description on the radio front panel accessories, the reader can refer to the *Front Panel Accessory Interface* section for the MOTOTRBO Mobile in [1].

3.1.2.5 Mobile Radio Rear Accessory and Peripherals Interface

Utilizing configurable GPIO pins for specific features requires programming with both MOTOTRBO CPS and MOTOTRBO Connect Plus CPS. First, MOTOTRBO CPS is used to assign the pin as a Generic Input or Generic Output. Then, MOTOTRBO Connect Plus Option Board CPS is used to configure the Generic Input or Generic Output for a specific feature. It is important to note that Connect Plus CPS does not know which physical pin number is used for the feature, and MOTOTRBO CPS does not know which Connect Plus feature is assigned to its physical pins. This means that the individual configuring the mobile and the Option Board must understand the big picture in order to configure both software programs correctly.

Connect Plus supports the following MOTOTRBO CPS configurable options:

Pin 17: Connect Plus supports “Generic Input 1” through “Generic Input 6”

Pin 19: Connect Plus supports “Generic Input 1” through “Generic Input 6” and “Generic Output 1” through “Generic Output 6”

Pin 20: Connect Plus supports “Generic Input 1” through “Generic Input 6” and “Generic Output 1” through “Generic Output 6”

Pin 21: Connect Plus supports “Generic Input 1” through “Generic Input 6” and “Generic Output 1” through “Generic Output 6”

Pin 22: Connect Plus supports “Generic Input 1” through “Generic Input 6” and “Generic Output 1” through “Generic Output 6”

Pin 24: Connect Plus supports “Generic Input 1” through “Generic Input 6” and “Generic Output 1” through “Generic Output 6”

Pin 26: Connect Plus supports “Generic Output 1” through “Generic Output 6”

Note the following:

- A single pin cannot be configured for both a Generic Input and a Generic Output.
- Once a pin is assigned as a Generic Input or Generic Output with MOTOTRBO CPS, a specific feature should be assigned to the Generic Input or Output using MOTOTRBO Connect Plus CPS.
- Connect Plus Supports the following features for Generic Inputs 1-6. Once a feature is mapped to a Generic Input, it cannot be used again:
    - External Mic PTT
    - Channel Select 1
    - Channel Select 2
    - Channel Select 3
    - Channel Select 4
    - Channel Select 5
- Connect Plus Supports the following feature for Generic Output 1-6. Once a feature is mapped to a Generic Output, it cannot be used again:
    - Horn and Lights (note: only Pin 26 supports 12v output for Horn and Lights)

3.1.2.6 Connect Plus Radio Configuration Requirements

Connect Plus uses the same MOTOTRBO portable and mobile radios as other digital modes. However, for Connect Plus operation these devices must meet several additional requirements, which are outlined as follows:

- The MOTOTRBO radio software version must be compatible with Connect Plus.
- A Motorola Option Board must be installed in the SU. Prior to the installation of Connect Plus software, the radio’s Option Board is referred to as a Generic Option Board (GOB). Following installation of Connect Plus software, the Option Board is referred to as Connect Plus Option Board.
- In order for the Connect Plus Option Board to enable its OTA interface and “talk” to the XRC controller, it must first verify that the Connect Plus feature has been enabled in the MOTOTRBO subscriber unit.

To program a radio for Connect Plus operation, two different versions of CPS programming software are needed:

- MOTOTRBO CPS is used to create zones and channels for Connect Plus use. See “Connect Plus System Design Considerations”, for a more detailed discussion of MOTOTRBO CPS programming guidelines.
- Connect Plus CPS is used for advanced configuration of Connect Plus parameters, including all of the following operations:

- Creating Connect Plus Contacts
- Assigning Channel Selector Knob positions (portable radio) or Channel Rocker positions (mobile radio)
- Entering Network, Site, & Frequency information
- Configuring Connect Plus feature options
- Configuring Connect Plus Menu Operation

3.1.3 User Interface & Ergonomics in Connect Plus

3.1.3.1 User Interface Dependencies

Because Connect Plus uses the same radio hardware as other digital modes, the physical buttons used by Connect Plus operation are the same as other digital modes. In some cases, however, these buttons operate differently for Connect Plus. All Connect Plus users should be aware of the following principles:

It is quite possible (in fact, it's likely) that the same programmable button will be used to activate different features, depending on whether the radio is selected to a Connect Plus channel or a non-Connect Plus channel.

- When selected to a non-Connect Plus channel, a programmable button operates as configured with MOTOTRBO CPS.
- When selected to a Connect Plus channel, programmable buttons operate as configured with Connect Plus CPS.

It is also important to note that Connect Plus is not aware of how a button has been programmed with MOTOTRBO CPS, and may not be aware of its current MOTOTRBO state (activated or de-activated). This can impact Connect Plus operation. For more information, see the following topics under "Connect Plus System Design Considerations":

- How MOTOTRBO CPS Button Settings Affect Connect Plus Operation
- How MOTOTRBO CPS Menu Settings Affect Connect Plus Operation

3.1.3.2 Connect Plus Buttons & Indicators

Push-to-Talk Button (PTT): In Connect Plus, if the radio is idle and monitoring the Control Channel timeslot when the user presses PTT, the SU will attempt to start a voice call using the Contact Name that has been programmed for the selected Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio). The contact name can either be a Group type (Group ID, Multigroup ID, Site All Call Group) or Private Call type. If it is a Group type, the radio attempts to start a Group Call to the programmed ID. If it is a Private Call ID, the radio attempts to start a Private Call to the destination Private ID. The SU sends a Call Request message on the Control Channel uplink. After transmitting the call request, the radio automatically de-keys in order to listen for the controller response. The radio user is usually unaware that the radio has keyed and de-keyed because he/she continues to press PTT while awaiting the talk permit tone. When the user hears the talk permit tone, this indicates that a channel has been granted and the user may begin to speak. If PTT is pressed during a call in progress (during the Call Hang Time), the radio begins transmitting audio to the assigned channel or slot. The

call request and set-up procedure does not apply in this case because the trunk-to slot has already been assigned.

Note: The Talk Permit tone is a programmable feature. When enabled via Connect Plus CPS (it is enabled by default), it can also be toggled on and off via the radio menu. Because Connect Plus is a trunking system, it is highly recommended to keep the Talk Permit tone enabled at all times. Otherwise, the radio user will not know when (and if) the controller has assigned a timeslot for the radio's transmission. When the Talk Permit tone is enabled, Connect Plus CPS also provides the ability to enable a "Pre-Tone". The purpose of the pre-tone (which is disabled by default) is to tell the radio user that the SU is in the process of call request. The Pre-Tone will be followed by a Talk Permit tone (if the channel is granted), a busy tone (if the call is placed in the Busy Queue) or a denial tone (if the request is denied for any reason).

Channel Selector Knob (portable) or Channel Rocker (mobile): In Connect Plus, each Channel Selector Knob position (for the portable radio) and the first 16 Channel Rocker positions (for the mobile radio) can be mapped to a specific Contact Name & Registration Group via CPS programming. The Contact Name determines what type of voice call is started when PTT is pressed. The Registration Group determines which Group ID the SU registers with when the knob or channel rocker is selected to that position. It is not allowable to assign some Channel Selector Knob (or Channel Rocker) positions to Connect Plus calls, and other positions to non-Connect Plus channels, within the same zone. To make a non-Connect Plus call, the user must change out of the Connect Plus zone, and then select the appropriate non-Connect Plus zone and channel. If the radio user selects an unprogrammed position for the Channel Selector Knob (mobile) or Channel Rocker (portable), the radio sounds a continuous tone and displays, "unprogrammed". The knob or channel rocker must be moved to a programmed position before the radio will be usable.

Programmable Buttons: Connect Plus CPS is used to configure how the radio's programmable buttons will operate when the radio is selected to a Connect Plus channel. The number of programmable buttons varies according to radio model. For each available button, the short press and long press can be programmed to operate differently. The orange button located on the top of the portable radio is commonly used to initiate and/or cancel an Emergency Alert or Emergency Call (depending on the Emergency mode configured for the selected zone), although it can be configured to function differently. If the radio is used for both Connect Plus and non-Connect Plus channels, then it is important to understand the interactions discussed in "User Interface Dependencies".

Status Indicators: Wherever possible, status indicators (LEDs, display, icons, tones, etc.) work in a similar fashion for both Connect Plus and non-Connect Plus channels. Some differences in operation are inevitable due to the nature of the radio-Option Board interface.

Menu System: When the radio is selected to a non-Connect Plus channel, the menu system is under the control of the radio's main board, and the programmable menu options are configured via MOTOTRBO CPS programming. When the radio is selected to a Connect Plus zone, the menu system is under the control of the Connect Plus Option Board, and the programmable menu options are configured via Connect Plus CPS programming. Wherever possible, Connect Plus attempts to duplicate the Menu structure and available options used on non-Connect Plus channels. Some minor differences are inevitable due to differences in Connect Plus operation and the nature of the radio-Option Board interface. The top-level Menu headings for Connect Plus are: Contacts, Scan, Zones, Messages, Call Logs, and Utilities. For details on these menus, see references [2] and [3].

Full keypad: The MOTOTRBO keypad portable with display offers a full numeric keypad for users to manually enter target addresses for system features. This keypad is also used as an alphanumeric keyboard for text messaging. The non-display portable does not come with a keypad. A mobile radio equipped with the standard microphone does not provide a means to compose text messages or manually enter target addresses for call features. As an option, the MOTOTRBO mobile offers an Enhanced Keypad Microphone so that users can compose text messages and manually enter target addresses for call features.

3.1.3.3 Connect Plus Voice and Emergency Feature Support

The following chart illustrates voice feature support for various MOTOTRBO models while selected to a Connect Plus channel.

Radio Model	Group Call	Multigroup Call	Site All Call	Private Call	Emergency Call	Emergency Alert
Display Portable	Yes	Yes	Yes	Yes	Yes	Yes
Non-Display Portable	Yes	Yes	Yes	Yes[32]	Yes[33]	Yes[34]
Mobile with full display	Yes	Yes	Yes	Yes	Yes	Yes
Mobile with numeric display	Yes	Yes	Yes	Yes[32]	Yes[18]	Yes[19]

To initiate a Multigroup Call, Site All Call, or Private Call the SU must be enabled for the call privilege in the controller's user database.

All models support reception of Network Wide All Call (NWAC), a one-way voice transmission initiated by a device (such as a digital wireline console) that connects to the Connect Plus network via the XRT Gateway. When a radio receives a NWAC, it is displayed on the receiving radio as a Site All Call

3.1.3.4 Connect Plus Command & Control Feature Support

The following chart illustrates which MOTOTRBO radio models can initiate various "Command & Control" call features.

Radio Model	Radio Check	Call Alert	Remote Monitor	Radio Enable	Radio Disable
Display Portable	Yes	Yes	Yes	Yes	Yes
Non-Display Portable	No	Yes[35]	No	No	No
Mobile with full display	Yes	Yes	Yes	Yes	Yes
Mobile with numeric display	No	Yes[35]	No	No	No

[32] For these models Private Call can be initiated by (a) assigning a One-Touch-Call to the Private Call ID or (b) assigning a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) for the destination Private Call ID. Private Call initiation via the Radio Menu is not available.

[33] These models have the ability to initiate an Emergency Call, but they do not have the ability to provide special ergo when receiving an Emergency Call. The *receive* ergo for these models will be the same as for Group calls.

[34] These models have the ability to initiate an Emergency Alert, but they do not have the ability to provide special ergo when decoding an Emergency Alert.

[35] Indicates the call type can only be initiated via a programmable "One Touch Call". Initiation via the menu is not available.

To initiate any of these call types, the SU must be enabled for the associated privilege in the controller's user database.

3.1.3.5 Analog Capability Not Available in Connect Plus

Connect Plus is a digital mode. Analog operation is not available while operating on a Connect Plus Channel. To activate analog capability, it is necessary to program the radio with a non-Connect Plus, analog capable, channel. This channel cannot be placed in any Connect Plus zone. It must be placed in a non-Connect Plus zone.

3.1.3.6 Connect Plus GPS Capability

Many radio models come equipped with an integrated, internal GPS receiver. Connect Plus supports Location Requests and Reports for radios that are so-equipped. For more information, see Connect Plus Location Services in the System Features section.

3.1.3.7 Connect Plus Text Messaging Compatibility

The following chart illustrates Text Message capability for various MOTOTRBO models while selected to a Connect Plus channel.

Radio Model	Receive Text Message?	Send Quick Text (programmed) Text Message	Create and send a limited free-form text message	Use a connected PC to create & send a text message
Display Portable	Yes	Yes	Yes	No
Non-Display Portable	No	Yes (if programmed for a One Touch Call)	No	No
Mobile with full display	Yes	Yes	Only if equipped with an optional Enhanced Keypad Microphone	No
Mobile with numeric display	No	Yes (if programmed for a One Touch Call)	No	No

If the radio is enabled for the "Route to PC" option with MOTOTRBO CPS, this will affect operation in non-Connect Plus channels only. Connect Plus Text Messages will not be routed to the PC.

3.1.3.8 Connect Plus Over-The-Air (OTA) File Transfer Capability

The following chart illustrates Connect Plus OTA File transfer capability for various models. OTA File Transfer is a Connect Plus feature not available in other digital modes.

Radio Model	Receive File via OTA File Transfer (for a supported file type)	Radio user can cancel transfer & start call	Utilities Menu displays “Current” & “Pending” Files[36]
Display Portable	Yes	Yes	Yes
Non-Display Portable	Yes	Yes	No
Mobile with full display	Yes	Yes	Yes
Mobile with numeric display	Yes	Yes	No

3.1.3.9 Vibrating Belt Clip

The Vibrating Belt Clip feature allows the user to select vibration as a type of notification for any "receiving" alerts, such as call alert, emergency notification and others. The portable radio must be installed with supporting hardware - battery and belt clip - to enable the feature functionality. The radio will automatically detect the attached battery and belt clip and will provide menu options on the display portable unit to configure Ring Alert Types with the following choices - Silent, Ring Only, Vibrate Only, Ring & Vibrate.

For display models, the Ring Alert Type programmable button can be assigned through CP CPS. Pressing the assigned programmable button will launch the Ring Alert Type menu, which allows the user to configure the ring alert type as previously described. For non-display models, when the user presses the programmable button the radio will update the setting to the next entry in the list.

The radio also provides three vibrate styles - Short, Medium and Long. For display models, the user can configure the Vibrate Strength option via a programmable button. Pressing the assigned programmable button will launch the Vibrate Style menu, which allows the user to configure the vibrate strength as previously described. For non-display models, when the user presses the programmable button the radio will update the setting to the next entry in the list.

This feature is supported only on the MOTOTRBO enhanced series portable radios. For more information, refer to the Connect Plus subscriber User Guide.

[36] Option Board Codeplug File displays “current” file only.

3.1.4 Connect Plus Data Applications

3.1.4.1 Application Server in Connect Plus

In other digital modes, a Data Application (such as a Text Message application or a Location application) resides on a PC that has a USB connection to a mobile radio, serving as Control Station. The Control Station radio acts as peer to other subscriber units in the field via the Common Air Interface. Connect Plus does not use this architecture. In Connect Plus, the Text Message or Location application resides on a PC that is connected via IP to a XRC Controller. This can be any Connect Plus controller on the radio network. The controller is the application's gateway to the Common Air Interface. This architecture provides significant advantages because the XRC Controller is the system component with the required knowledge to locate the destination SU, identify an available RF resource, and deliver the message to its intended target.

3.1.4.2 Connect Plus Presence Notifier

Data applications work best when they know whether the Destination Connect Plus SU is currently registered (or not registered) to the Connect Plus network. This knowledge allows the application to operate efficiently and to conserve IP bandwidth.

In other MOTOTRBO digital modes, subscriber radios report their presence in the network by using the Automatic Registration Service (ARS) protocol to communicate with the MOTOTRBO Presence Notifier or a third Party ARS application. The Connect Plus SU does not use ARS to report its presence in the network. Instead, Connect Plus uses short messages that are sent on the Control Channel as part of the normal procedure for registering or de-registering with the XRC Controller.

In Connect Plus, a data application may obtain presence information by subscribing to the Connect Plus controller, acting as Presence Notifier. In doing so, the data application utilizes Motorola's Presence Notifier-to-Watcher Interface Specification, with some modifications as specified for Connect Plus. This allows the data application (the "Watcher") to request presence information for specific SU's. The XRC notifies the Watcher when the specified SU registers or de-registers from the Connect Plus network.

3.1.4.3 Multi-Channel Device Driver (MCDD) in Connect Plus

The Multi-Channel Device Driver (MCDD) is **not** used in Connect Plus. In Connect Plus, a data application can send its message to any XRC controller in the network. The application does not need to be concerned about what site or channel the destination SU is currently using. Tracking the SU between sites is the responsibility of the XRC controller. If the SU is not registered to the controller that received the message, the controller forwards the message to the controller of the SU's registered site.

3.1.4.4 Text Message Application, Server & Client in Connect Plus

While Connect Plus supports third party text message applications (including server & client operations), the Motorola MOTOTRBO Text Messaging application is not currently supported. To determine whether a specific third party application supports Connect Plus operation, contact the vendor. The vendor can also supply specifications for the computer platform necessary to run the application. For general information about how third party text applications work in Connect Plus, see "Connect Plus Text Messaging" in the System Feature section.

3.1.4.5 Location Tracking Application, Server & Client in Connect Plus

While Connect Plus supports third party text Location tracking applications (including server & client operations), the Motorola MotoLocator tracking application is not currently supported. To determine whether a specific third party application supports Connect Plus operation, contact the vendor. The vendor can also supply specifications for the computer platform necessary to run the application. For general information about how third party Location applications work in Connect Plus, see "Connect Plus Location Services" in the System Feature section.

3.2 Connect Plus System Topologies

3.2.1 Direct Mode

Direct Mode, where one SU communicates directly to another SU without using a MOTOTRBO repeater, is not available in Connect Plus. A Connect Plus SU can only communicate with other SU's via MOTOTRBO Repeaters and the XRC controller. To set-up Direct Mode, it will be necessary to program the SU with at least one non-Connect Plus zone and channel. While the radio is selected to the Direct Mode channel, the SU will not hear any Connect Plus calls. When programming the Direct Mode frequency, do not program any Connect Plus repeater frequency. Otherwise, the Direct Mode transmission may interfere with Connect Plus operation.

3.2.2 Repeater Mode

The MOTOTRBO repeater is a required component of the Connect Plus trunking system, as it provides the RF path between the Connect Plus Controller and the Connect Plus SU. Furthermore, Connect Plus SU's never speak to each other in Direct Mode (while selected to a Connect Plus personality). Connect Plus transmissions pass through one or more MOTOTRBO repeaters and one or more XRC controllers (depending on whether the SU's are located at the same site or at different sites).

In Connect Plus, the repeater operates in digital mode, thereby providing all of the advantages of digital signaling (two timeslots, error correction, etc.). In addition, Connect Plus offers the additional benefits of trunked operation. In conventional operation, each position on the SU's Channel Selector Knob (portable radio) or Channel Rocker (mobile radio) is assigned a specific repeater and timeslot via CPS programming. If the repeater timeslot is busy with another call, the radio user is blocked from communicating until the timeslot becomes available. In Connect Plus, the SU makes the Call Request on the Control Channel timeslot, and the controller can assign the call to any available repeater and timeslot in the site. While this requires a dedicated timeslot for Control Channel signaling, it also greatly reduces call blocking. Calls are not blocked until all of the site's repeaters and timeslots are busy. Even then, the Controller will continue to receive Call Requests and place them in the Busy Queue. When a timeslot becomes available, the controller assigns the highest priority call from the Busy Queue. When priorities are equal, calls are assigned on a first-in, first-out basis.

Just as in other MOTOTRBO digital modes, all MOTOTRBO repeaters that have overlapping coverage must be programmed with different frequency pairs so as not to interfere with one another. Frequencies may be re-used when coverage does not overlap. If coverage does not typically overlap, but may in certain conditions (such as when the SU is in a very high place), the re-used frequencies must have different Color Codes. This will not eliminate interference between the two repeaters, but it will help SU's distinguish between the different repeaters – especially while roaming.

In other digital modes, the MOTOTRBO repeater processes calls without the involvement of any additional device, such as a controller. In Connect Plus, both the MOTOTRBO repeater and the XRC controller are involved

in every Connect Plus call. For more information about how the Connect Plus system uses the MOTOTRBO Repeater and how calls are processed, see the following sections:

- Connect Plus Features (and its sub-sections)
- Connect Plus System Components and Topologies: Repeater Operation in Connect Plus
- Connect Plus System Design Considerations: Multiple Digital Repeaters in Connect Plus Mode

3.2.3 Topologies of a Connect Plus System

Connect Plus system topologies fall into two major categories:

- Connect Plus Single Site System
- Connect Plus Multisite Network

3.2.3.1 Connect Plus Single Site System

A Connect Plus Single Site System provides multi-channel trunking capability to a single geographical area. The size of the geographical is determined by factors such as:

- Propagation characteristics of RF band utilized
- Height of site antenna(s) and repeater power output
- RF output & antenna efficiency of mobile and/or portable radio devices
- Type of terrain and other obstructions (buildings, etc)

The essential components of a Connect Plus Single Site System are:

- XRC Trunking Controller
- 1-15 MOTOTRBO Repeaters. All repeaters under the control of the same XRC controller must reside in the same RF frequency band and must all have an identical coverage footprint (both “talk in” and “talk out”).
- Ethernet Switch to connect XRC Controller with repeaters
- Other Site Equipment to include
  - RF Equipment such as combiners, RF cables, antenna(s), etc.
  - Power backup for the XRC controller
  - Power backup for MOTOTRBO Repeaters
- MOTOTRBO portable and/or mobile radios (including antennas, microphones, etc). These MOTOTRBO SU’s may be located anywhere within the RF coverage of the Connect Plus site.

The optional components of a single-site Connect Plus Single Site System are:

- A second XRC Controller to serve as redundant backup to the primary Controller
- PC with Location Tracking application
- PC with Text Messaging application
- PC with RDAC application for repeater monitoring and alarm reporting
- In Connect Plus, the above applications communicate with the Connect Plus System via IP connection to the XRC controller. The computer hosting the application can be co-located with the controller, or it can be in a different location. If the computer is in a different location, a Backend IP network is needed to connect the XRC with the PC hosting the application. A Backend network is also needed if the System Administrator wishes to remotely access the Controller via IP using a PC running the MOTOTRBO Connect Plus Network Manager software.
- XRT Gateway, a device that allows certain 3rd party client applications to interface with the Connect Plus System. For more information, see the "XRT Gateway" section.

3.2.3.2 Connect Plus Multisite Network

Connect Plus Multisite Networking is a purchasable option. Multisite Networking refers to the ability to interconnect multiple Connect Plus single-site systems. In the initial release, up to six single-sites can be joined together to form a Connect Plus network.

The most common reason for connecting multiple sites is to enlarge the RF coverage available to the Connect Plus SU. Because of this, each Connect Plus site is typically placed in a different geographical area and provides the RF coverage for that area. As the radio user moves from one coverage area to another, the SU is able to automatically "Roam" from one site to another. Whenever the SU registers with a different site, the controller forwards information on the SU's whereabouts to all other controllers. This allows all network controllers to "track" the SU as it moves it around the network. The registration process not only tells the controller which SU is registering with the site, it also tells the controller which Talk Group the user has selected for communications. When the radio user wishes to communicate with other SU's, the XRC controllers will transmit the call at any network site where the Destination ID is currently registered. It should be noted that even in a multisite network, each site is still controlled by its local XRC Controller. A controller can assign a call to any repeater within its own site, but it cannot assign a call to another site's repeater without the permission and involvement of that site's controller. A controller can "trunk" SU's to any repeater in its own site, but it cannot "trunk" an SU to a repeater in a different site. The SU must "roam" to the new site after it loses signal from the current site.

A less common reason for linking multiple Connect Plus sites is to provide communications between MOTOTRBO radios that use different frequency bands. In this case, each frequency band requires its own Connect Plus site. The Connect Plus sites in different frequency bands can be geographically separated or they can be co-located.

Because a Connect Plus network is essentially a collection of interconnected single-sites, the list of single-site essential components (from the previous section) also applies to each site in the multisite configuration. In addition to these, multisite operation requires several other "essential" elements. They are listed as follows:

- Each site requires its own XRC controller, and each XRC must be enabled for the purchasable multisite permission.

- Each controller must be configured with several additional parameters that are not used in the single-site, stand-alone configuration. These parameters tell the controller how to communicate with the other networked controllers, what timer value to use for call arbitration, and they also tell the controller what "Neighbor Site" information should be transmitted over-the-air to the listening SU's.
    - **Note**: Each entry in the Multisite table must be actual/physical XRC or XRT installed and operational on the IP network. Pre-configuring the Multisite table with sites planned for future expansion (i.e. sites that do not currently exist) **must be avoided.** Adding non-existent sites to the Multisite table may drastically hinder controller's performance.
- Because the XRC controllers communicate via TCP/IP and UDP/IP, there must be a Backend IP Network to connect the different sites. Network IP configurations and bandwidth requirements are discussed in other sections of this System Planner.

The optional components of a Connect Plus Multisite Network are very similar to the optional components of a stand-alone single-site:

- A second XRC Controller to serve as redundant backup to the primary Controller.
- PC with Location Tracking application. It can be connected via IP to any XRC controller in the network. The connected controller will inspect the incoming messages, and forward them to other site controllers, if necessary. While it's not required to have multiple Location Tracking applications connected to different sites, there are scenarios where the customer's requirements may warrant such a configuration.
- PC with Text Messaging application. It can be connected via IP to any XRC controller in the network. The connected controller will inspect the incoming messages, and forward them to other site controllers, if necessary. While it's not required to have multiple Text Messaging applications connected to different sites, there are scenarios where the customer's requirements may warrant such a configuration.
- PC with RDAC application for repeater monitoring and alarm reporting. Earlier versions of RDAC supported just one IP Site Connect System (i.e. one Connect Plus site) per instance of the RDAC application. Newer versions of RDAC can communicate with more than one IP Site Connect Master. This means that newer versions of RDAC can be configured to monitor multiple IP Site Connect Systems (i.e. multiple Connect Plus sites) from a single instance of the RDAC application. However, any Connect Plus site managed by the RDAC application (whether a single Connect Plus site or multiple Connect Plus sites) must reside in the same LAN or VPN as the PC running the RDAC application.
- Up to five XRT Gateways. The XRT Gateway is a device that allows certain 3rd party client applications to interface with the Connect Plus System. For more information, see the "XRT Gateway" section.

3.2.4 Network IP Topologies for Connect Plus System

The devices in a Connect Plus network (with the exception of the subscriber radios) communicate with one another via IP messages received on their Ethernet port(s). It follows that these devices will each have an IP address and will be need to be connected via some type of IP network. This section will discuss various IP topologies of the Connect Plus System.

The IP network topologies can be divided into two primary configurations:

- Local Area Network
- Wide Area Network

Some customers will have network topologies that are combinations of these configurations.

3.2.4.1 Local Area Network (LAN) Configuration

Customers that have high capacity network connectivity throughout their organization will most likely have a desire to utilize their existing infrastructure for wide area connectivity. Connect Plus supports the following technologies:

- Private LANs
- Corporate LANs
- Private Wireless LANs (e.g. Canopy or Point-to-Point (PTP), 802.11/Wi-Fi network)

Sometimes Private Wireless network installations utilize topologies which include redundant point-to-point links for increased communication reliability. It is the customer's responsibility to configure and test such network prior to deploying the Connect Plus equipment. It is necessary to note that networks with redundant links will still affect the inter-site controller communication in an event of a primary link failure. Depending on the network devices providing the redundant functionality such link downtime can vary from several seconds to minutes.

Typically, with equipment and systems operating over IP networks, there is dedicated personnel responsible to maintain the integrity of the network and the security of the connected IP hosts. IT professionals often employ network probing tools with port scanning functions. It is strongly advised to **avoid** executing any prolonged and extensive port scans on the Connect Plus infrastructure components, namely XRC, XRT, XRI and repeaters.

The Local Area Network configurations can have many variations. As long as the devices are on the same network, or have access to other networks through an internal router or NAT configurations, the Connect Plus system will operate correctly. It is also assumed that in these local configurations that bandwidth is not an issue. The diagram below shows a simple diagram of Connect Plus sites connected through a local area network.

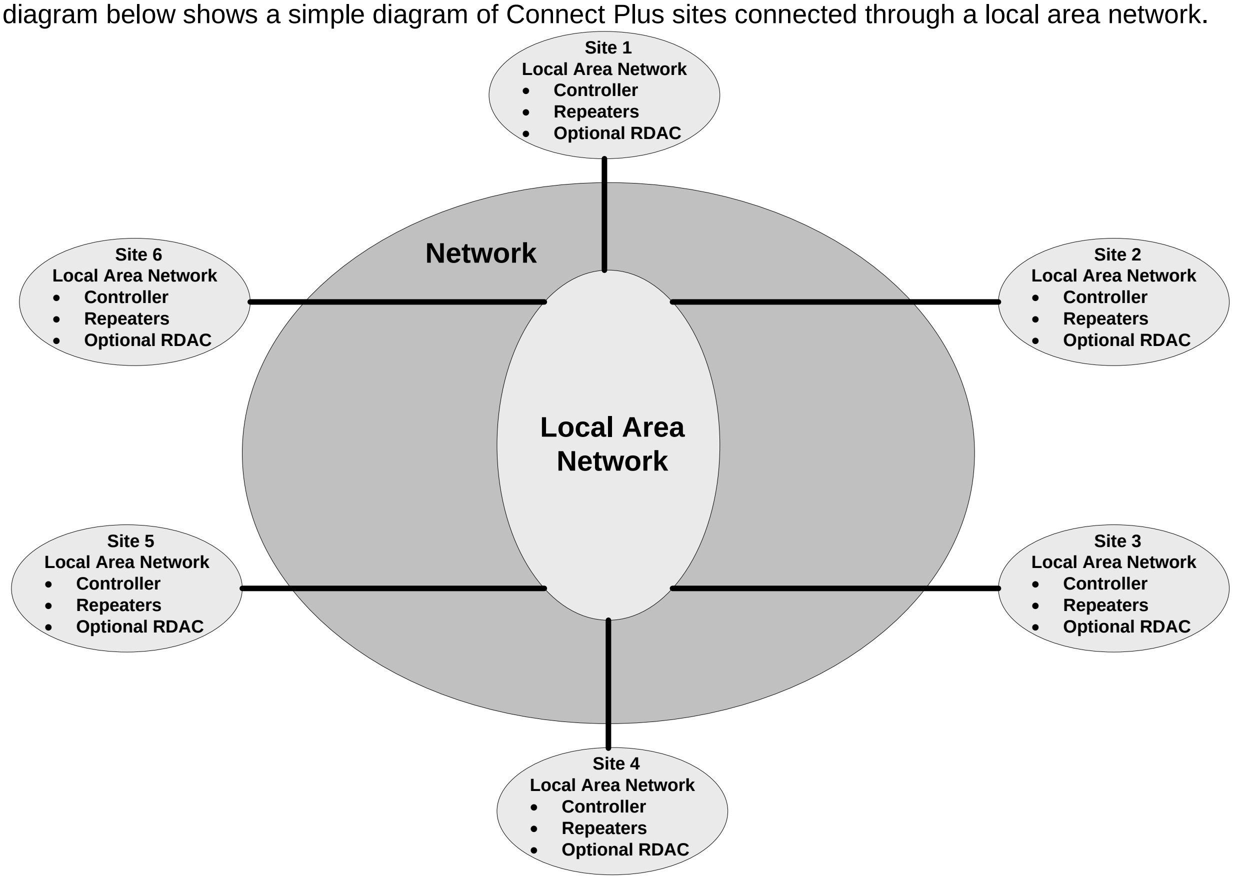


Figure 3-1 Connect Plus Sites Connected through LAN

3.2.4.2 Wide Area Network (WAN) Configuration

One of the values of Connect Plus is the ability to connect sites over public Internet Service Provider (ISP) links as well as private broadband connections. ISPs provide a range of technologies with varying bandwidth. Connect Plus supports the following technologies (as long as the requirements listed in the backend Network Considerations section are met):

- Private T1
- DSL/ADSL
- Cable Modem
- Broadband Wireless Access
- ISDN
- Frame Relay

⚠ For all the types of network links listed above it is **strongly** recommended to establish a commercial grade of service with the ISP in order to ensure reliability required for real-time packet based communication systems such as Connect Plus. For discussion on backend network characteristics the reader is encouraged to review section Considerations for the Connect Plus Backend Network.

Connect Plus does not support dial-up connections (due to small bandwidth) or Satellite Internet access (due to large delay). When utilizing public internet connections, it is important that the system installer understand the bandwidth and delay that each Connect Plus device requires in order to operate optimally. They must also understand the details (bandwidth and delay) of the network link at each site and between sites. For example, if connecting sites have long distances between them, the delay of the entire link needs to be considered.

A Connect Plus site can be (and is suggested to be) behind a router and/or a NAT and/or a firewall. Although not required, it is highly suggested in order to protect against the undesired solicitations common over the public internet. Although Connect Plus should work through most off-the-shelf devices, the following router/NAT/firewalls have been validated with Connect Plus:

- HP ProCurve 7102dl Secure Router[37]
- HP A-MSR20-20 Router (JF283A)[38]
- HP MSR2003 Router (JG411A)
- Cisco 2911 Integrated Services Router

The network equipment market offers devices labeled as “Layer 3 switches”, which in addition to the Layer 2 MAC frame-based switching, perform IP packet routing/forwarding, i.e. such devices act as routers. It is important to note that Connect Plus has **not** been specifically verified or tested with Layer 3 switches, but there would be no reason to discourage such equipment use in Connect Plus system deployments. However, it is strongly recommended to utilize the skills of seasoned IT technicians familiar with these devices to ensure proper provisioning.

For the first release Connect Plus provides TCP authentication, but no IP encryption features. For customers that are concerned with such privacy matters, and want to protect the system traffic over the IP networks it is recommended to employ a Secure VPN layer. Secure VPN is not a function of the Connect Plus device but rather of the router. It is important to note that VPN does add the need for additional bandwidth and may introduce additional delay. This should be taken into consideration in bandwidth planning. The following router is recommended for establishing secure VPN links between the Connect Plus sites.

- HP A-MSR20-20 Router (JF283A)
- HP MSR2003 Router (JG411A)

[37] The **7102dl** router has reached “End of Sale” and may not be available for purchase at the time of this publication.
[38] The **MSR20-20** router has reached “End of Sale” and may not be available for purchase at the time of this publication.

Additionally, the following Secure VPN router has been used with other MOTOTRBO system installations, but has not been officially validated on Connect Plus:

- Linksys 4 Port Gigabit Security Router with VPN: Model RVS4000

Each XRC controller requires a static IPv4 address from the Internet Service Provider. The other Connect Plus controllers utilize this static IPv4 address to establish their link with the wide area system.

The diagram below shows a simple diagram of Connect Plus sites connected through a wide area network.

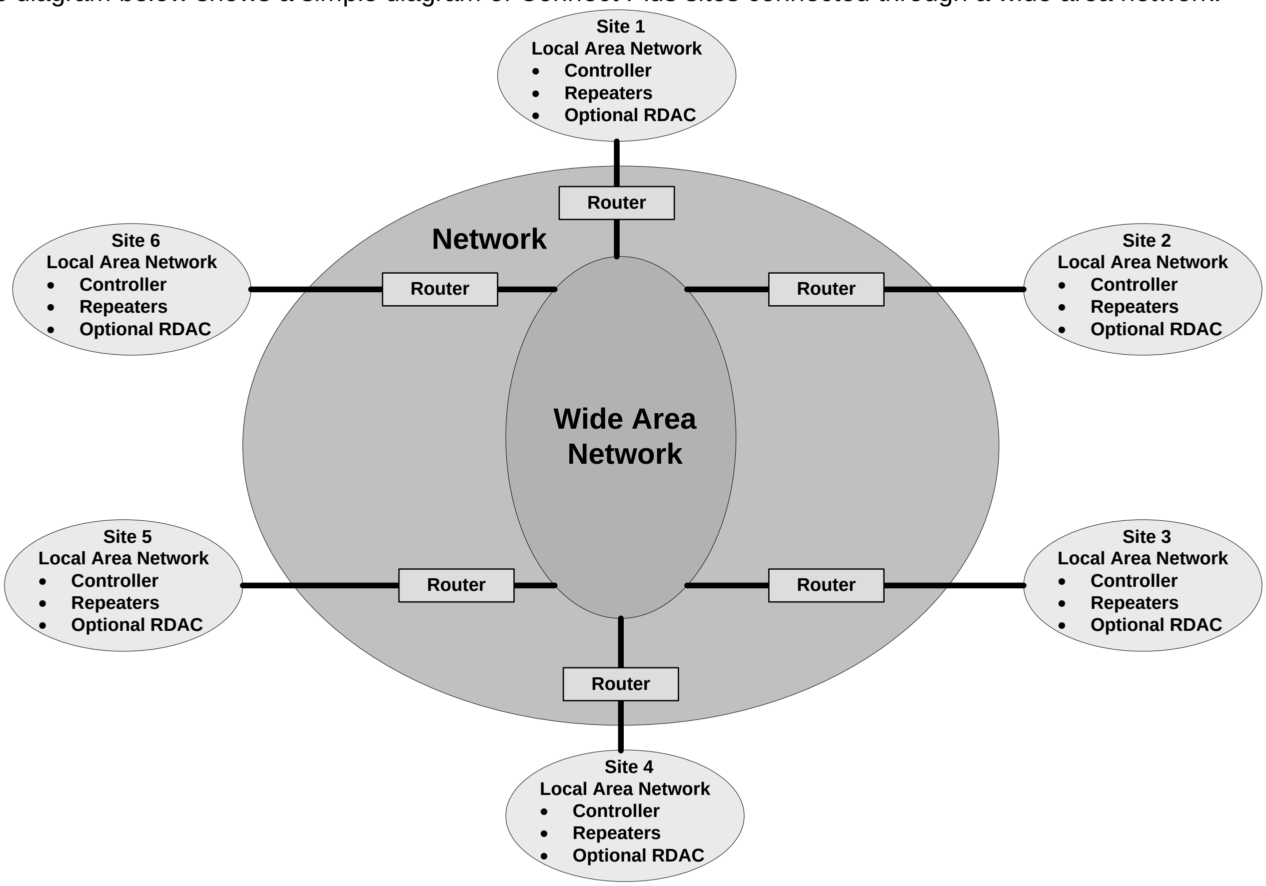


Figure 3-2 Connect Plus Sites Connected through WAN

3.2.4.3 IP Topologies of a Single Site System

An example of a Connect Plus Single Site system configuration is illustrated in Figure 3-3.

XRC Controller and MOTOTRBO Repeaters: Because the XRC controller and the MOTOTRBO repeaters under its control must be in the same physical location and connected to the Ethernet switch, these devices will be on the same Local Area Network (LAN). The following Ethernet switches have been validated with Connect Plus:

- HP ProCurve 2510-24 ([39])
- HP 2530-24
- Cisco Catalyst 3560

[39] The **2510-24** Ethernet switch has been scheduled for "End of Sale" by HP and may not be available for purchase at the time of this publication.

RDAC Application: If RDAC capability is desired for error reporting, the PC hosting the RDAC application must be in the same LAN (or VPN) as any Connect Plus site being managed by RDAC. The reason is as follows: RDAC communicates with the XRC and with the site's repeaters via the Link Establishment (LE) Protocol. The Controller is the LE Master. The MOTOTRBO repeaters and the RDAC application are LE Peers. If Peers are ever located in different networks, then all peers must address the Master via its publicly addressable IP, not its local IP address. This even applies to the peers that are in the same LAN as the Master. This requires a router capable of a special feature called "hair-pinning", which turns the messages around to send them back to the Master (in this case, the XRC controller). Due to the time sensitive nature of the messaging between the XRC controller and its peer repeaters, the latency added by this additional routing and the hair-pin address conversion will be detrimental to system performance. For this reason Connect Plus requires all Peers, including RDAC, to be located in the same Local Area Network (LAN) or Virtual Private Network (VPN) as the XRC controller acting as Master.

Location Tracking Application: If a Location Tracking Application is desired, the PC hosting the application can be located in the same LAN as the XRC controller, or in a different LAN.

Text Messaging Application: If a Text Messaging Application is desired, the PC hosting the application can be located in the same LAN as the XRC controller, or in a different LAN.

MOTOTRBO Connect Plus Network Manager Software: A PC hosting the MOTOTRBO Connect Plus Network Manager software can connect to XRC either locally or remotely. For remote connections, the PC hosting the MOTOTRBO Connect Plus Network Manager program can be located in the same LAN as the XRC controller, or in a different LAN.

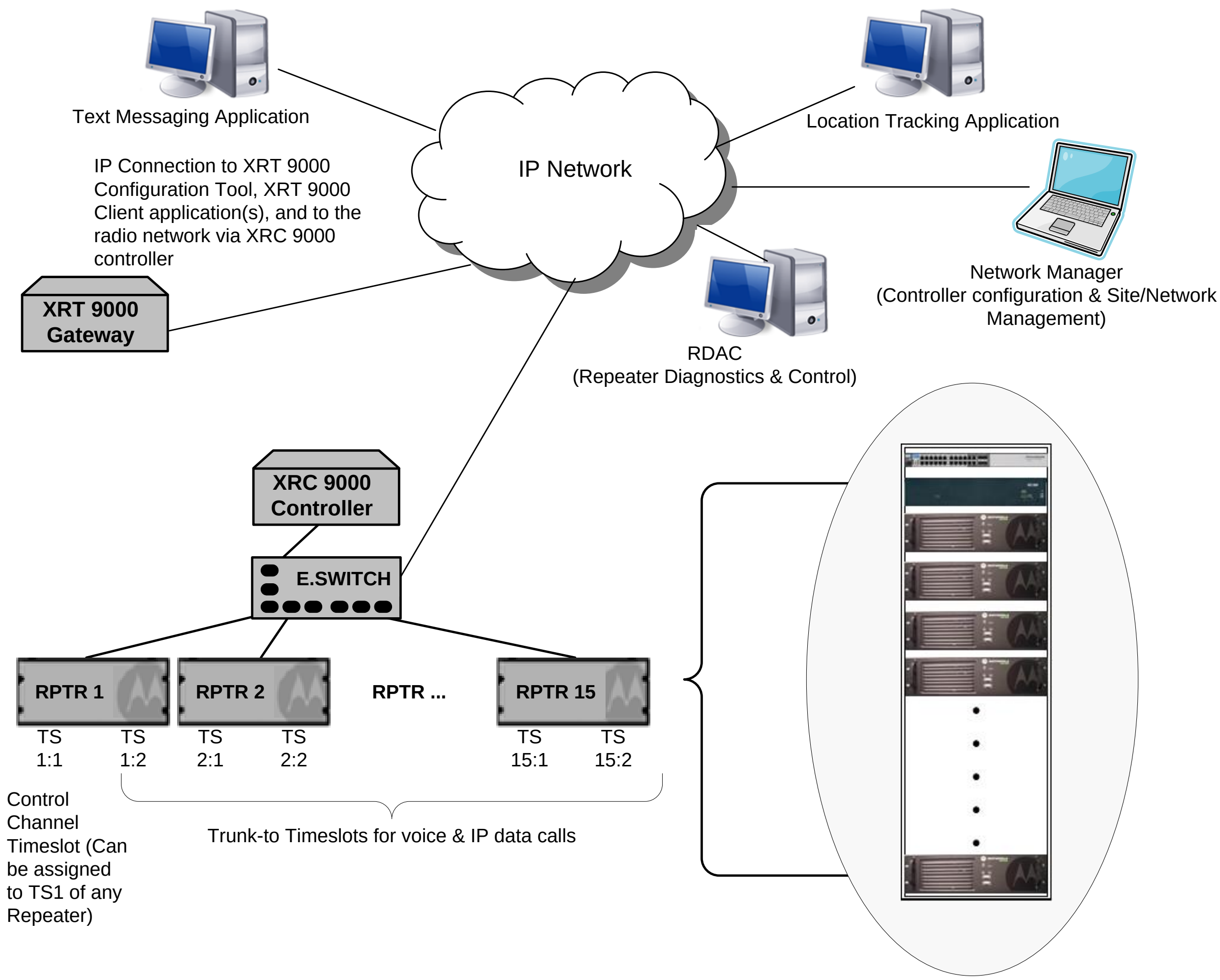


Figure 3-3 Connect Plus Single Site Configuration

XRT Gateway: Allows certain 3rd party client applications to interface with the Connect Plus System. The XRT Gateway can be located in the same LAN as the XRC controller, or in a different LAN.

3.2.4.4 IP Topologies of a Multisite Connect Plus Network

A multisite Connect Plus Network consists or multiple Connect Plus single-sites that are networked together via an IP backbone. The sites communicate with one another via TCP/IP and UDP/IP. An example of a Connect Plus Multisite system configuration is illustrated in Figure 3-4.

XRC Controller and MOTOTRBO Repeaters: As stated in the previous section, the XRC controller and its connected site repeaters are always in the same LAN.

XRC Controllers located at different sites: In a multisite network, the repeaters communicate only with their local XRC controller. They do not exchange messages with controllers or repeaters at other Connect Plus sites. Instead, all network communications are handled by the XRC controllers. These controllers can all be in the same network, in different networks, or a combination of both.

The recommended multisite topology, wherever possible, is that the all XRC controllers should reside in the same private network or virtual private network (VPN). There are some important reasons for this recommendation:

- Regardless of what network configuration is utilized, the network links must meet the bandwidth, latency, and jitter requirements discussed in Connect Plus System Design Considerations. In a Private IP Network the amount of IP traffic, network capacity, and message routing is under the control the network owner. Because of this, the private network can be designed to ensure adequate Connect Plus bandwidth and performance. In public networks, capacity, loading and routing tend to be more unpredictable. This makes it more difficult to assure that Connect Plus requirements can be consistently met.

- In Private or Virtual Private Networks, each XRC controller can communicate with one another directly, using IP addresses that are known and consistent network wide. This greatly simplifies the required IP set-up, both in the XRC controllers and in the network's routers. When the XRC controllers reside in multiple IP networks, the IP configuration is not as straight-forward.

- Private networks have advantages in the important area of IP security. Connect Plus supports the ability to work through a Secure VPN (Virtual Private Network). Secure VPN is not a function of the XRC controller device but rather of the router. It is important to note that VPN does add the need for additional bandwidth and may introduce additional delay. This should be taken into consideration in bandwidth planning.

While it is highly desirable to exclusively utilize private IP links, this may not be possible for all customers. Connect Plus has been designed to accommodate different types of network configurations, including the ability to connect sites over public Internet Service Provider (ISP) links.

Connect Plus is also designed to work in a mixed IP network environment. Examples of a mixed IP network environment include the following:

- Some sites reside in a private IP network, while others reside in a public IP network

- Some sites reside in public IP network “A”, while others reside in public IP network “B”

Mixed IP network topologies significantly complicate IP address set-up, port configuration, router configuration, and IP security issues.

Regardless of whether Connect Plus sites are linked via private or public connections, the following requirements must be fulfilled for all Connect Plus IP links:

- Each Connect Plus Controller requires a static IP address. In a public network, the static address is provided by ISP (Internet Service Provider).

- Regardless of what network configuration is utilized, the network links must meet the bandwidth requirements discussed in Connect Plus System Design Considerations.

- Connect Plus sites communicate exclusively via TCP/IP and UPD/IP. If a linking technology converts these messages to a different format for transport, they must be converted back to TCP/IP and UDP/IP prior to being delivered to the XRC Controller at the destination site. If any conversion is done, the process must be completely transparent (invisible) to all XRC controllers. Furthermore, the conversion process must not prevent the network link(s) from meeting the bandwidth requirements discussed in Connect Plus System Design Considerations.

- Connect Plus does not support dial-up connections for inter-site messaging (due to small bandwidth) or Satellite Internet access (due to large delay).

- Network security is an important consideration. In the event that Connect Plus sites will be connected through anything other than a Private Network or Virtual Private Network, a Certified Networking Professional will need to assist the system owner in protecting the radio network from the undesired solicitations common over the public internet.

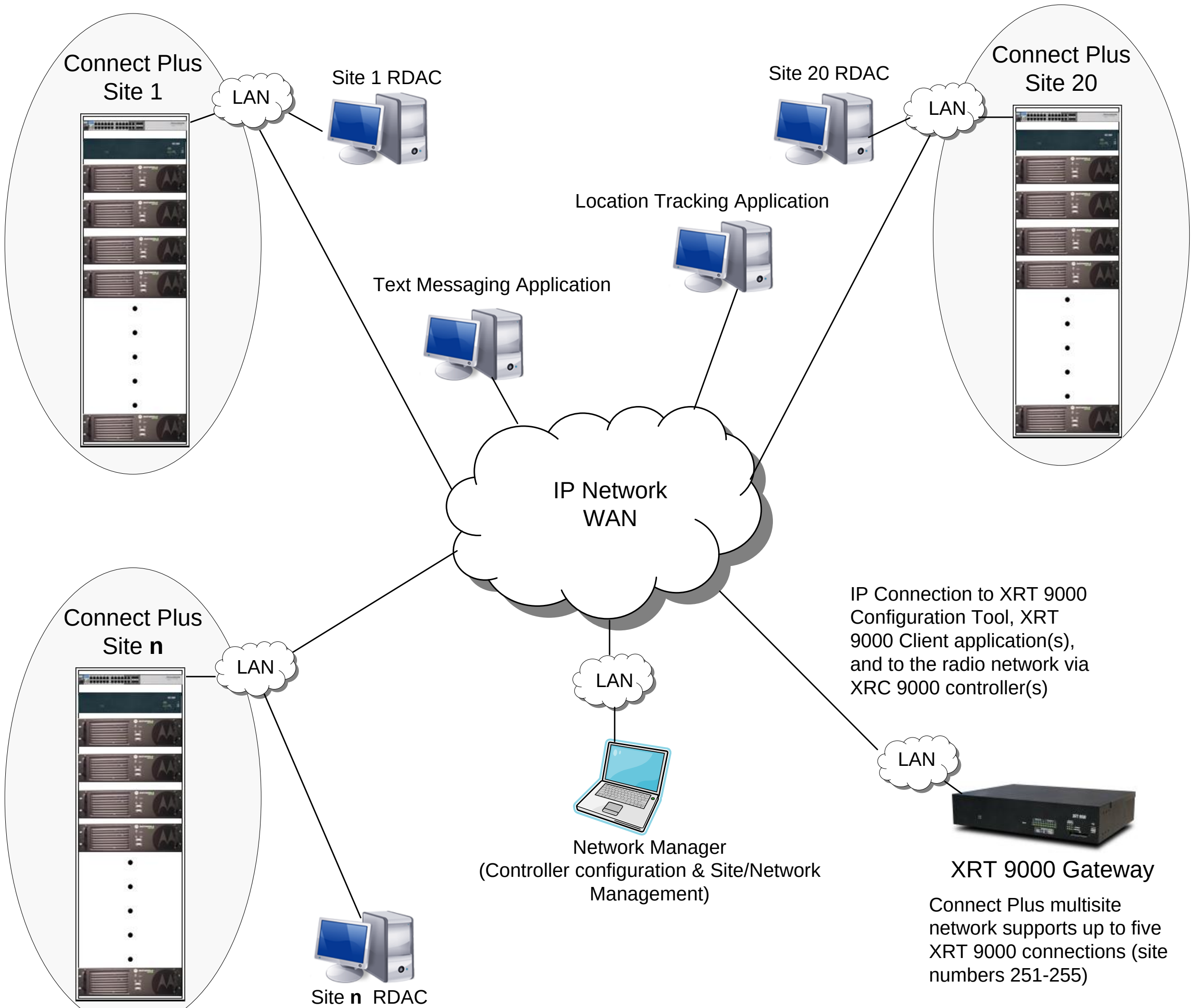


Figure 3-4 **Connect Plus Multisite Configuration**

3.2.4.5 Other IP Components of the Connect Plus Multisite Network

RDAC application: As discussed previously, the RDAC application must reside in the same LAN (or VPN) as its Link Establishment (LE) Master (the XRC controller) and its LE Peers (the MOTOTRBO repeaters under the control of the XRC Controller.) If the RDAC application is managing multiple Connect Plus sites, then all sites managed by the RDAC application must be in the same LAN (or VPN) as the PC running the RDAC application. For more information on the reasons for this requirement, please see the previous section *IP Topologies of a Single Site System*.

Location Tracking Application: If a Location Tracking application (also known as the LRRP application) is utilized in the Connect Plus multisite network, it can send the Location Request to any Connect Plus site controller. The PC hosting the requesting application can be located in the same IP network as the destination site, or in a different IP network. The XRC controller that receives the message will inspect the message contents to determine the destination SU. If the SU is registered at a different network site, the XRC controller will forward the message to the registered site. The registered site, upon receiving the Location Report from the SU, sends it directly to the requesting application. It does not route the report back through the Connect Plus site that received the request.

When a Connect Plus controller sends a message to the Location application, the IP address and port used by the controller depends on how the controller is programmed. There are two configuration choices:

- **Method A**: Controller is <u>not</u> programmed to use a LRRP Server IP address and port that has been configured into the controller. In this case, the controller sends the Location Report to the source IP address and port extracted from the LRRP Request that prompted the report.

- **Method B**: Controller is programmed to use a LRRP Server IP address and port that has been configured into the controller In this case, the controller sends the Location Report to the address and port configured into the controller. This feature is known as LRRP IP Message Forward, also known as the "override" function.

Method A is the default Controller operation. It provides more flexibility than Method B because it supports a different Location Tracking application for each SU. However, it can only be used when all network sites have the same perspective back to the requesting application. The following example describes one scenario where all network sites would <u>not</u> share the same perspective. The Location application and Site 1 are both located in the same LAN. The Location application sends a message to Site 1. Site 1 inspects the message and sees that the destination SU is registered at Site 2. Site 1 forwards the message to Site 2, which is located in a different IP network. The forwarded message is wrapped inside of a Connect Plus TCP inter-site message. Site 2 sends the Request to the SU and receives a Location Report. When Site 2 sends the Location report back to the requesting application, it must not use the Source IP address and port extracted from the request because that is the application's "private IP address" on its LAN, and it will not be correct from the perspective of Site 2. Instead, Site 2 must use the application's "public IP address" and port. Since this cannot be known by inspecting the contents of the received message, Site 2 must be enabled for "override" and must use its configured "LRRP IP Message Forward" address and port. This is just one example where Method B must be used. Other scenarios could also necessitate this approach. Method B provides less flexibility than Method A because there is just one configurable LRRP Server IP address and port per site. This means that all SU's must report to the same Location tracking application.

Text Message Application: If a Text Message application (also known as the TMS application) is utilized in the Connect Plus multisite network, it can send the TMS message to any Connect Plus site controller. The PC hosting the requesting application can be located in the same IP network as the destination site, or in a different IP network. The XRC controller that receives the message will inspect the message contents to determine the destination SU. If the SU is registered at a different network site, the XRC controller will forward the TMS message to the registered site. If the TMS message was a "Simple Text Message", the site forwards the

message to the destination SU. If the TMS message was a “TMS Service Availability” Message, the site stores the information contained in the message on behalf of the destination SU.

When a Connect Plus SU wants to send a simple text message to a Dispatch Call ID (which represents a “client” of the TMS application), the SU sends the message to the controller of the site where the SU is registered. The message contains the destination Dispatch Call ID, but it does not contain the IP address of the Text Message application. The SU counts on the controller to forward the message to the correct IP address and port for the TMS application. When the controller forwards to the simple text message to the TMS application, the IP address and port used by the controller depends on how the controller is programmed. There are two configuration choices:

- **Method A**: The controller is not programmed to use a TMS Server IP address and port that has been configured into the controller. In this case, the controller sends the simple text message to the source IP address and port extracted from the TMS Service Availability Message, which the controller stored on behalf of the SU.

- **Method B**: Controller is programmed to use a TMS Server IP address and port that has been configured into the controller. In this case, the controller sends the simple text message to the address and port configured into the controller. This feature is known as TMS IP Message Forward, also known as the “override” function.

Method A is the default Controller operation. It provides more flexibility than Method B because it supports a different TMS application for each SU. However, it can only be used when all network sites have the same perspective back to the TMS application. The following example describes one scenario where all network sites would not share the same perspective. The TMS application and Site 1 are both located in the same LAN. The TMS application sends a TMS Service Availability Message to Site 1. Site 1 inspects the message and sees that the destination SU is registered at Site 2. Site 1 forwards the message to Site 2, which is located in a different IP network. The forwarded message is wrapped inside of a Connect Plus TCP inter-site message. Site 2 stores the information contained in the message on behalf of the destination SU. Sometime later, the SU sends the controller a simple text message which is destined for a Dispatch Call ID. When the controller forwards this simple text message to the TMS application, it must not use the Source IP address and port extracted from the TMS Service Availability Message because that is the application’s “private IP address” on its LAN, and it will not be correct from the perspective of Site 2. Instead, Site 2 must use the application’s “public IP address” and port. Since this cannot be known by inspecting the contents the TMS Service Availability message, Site 2 must be enabled for “override” and must use its configured “TMS IP Message Forward” address and port. This is just one example where Method B must be used. Other scenarios could also necessitate this approach. Method B provides less flexibility than Method A because there is just one configurable TMS Server IP address and port per site. This means that any text message from any SU that is addressed to any Dispatch Call ID will be forwarded to the same TMS server.

MOTOTRBO Connect Plus Network Manager Connection Tool & **MOTOTRBO Connect Plus Network Manager**: The MOTOTRBO Connect Plus Network Manager Connection Tool is used to establish connection(s) with Connect Plus Site(s), and to authenticate the entered Username and Password. The connection can be a serial connection (to one site at a time) or a TCP/IP connection (to a single site, or to multiple sites).

For TCP/IP connections, the destination XRC can be located in the same IP network as the PC hosting the Connection Tool application, or in a different IP network. In order to connect with a desired site, the Connection Tool must be configured with a destination IP address and port that is correct from the current perspective of the PC hosting the application. If the PC is a laptop, this perspective can change as the laptop is carried from one IP network to another. So, depending on its location, the laptop may not always use the same IP address and port to connect to the same site.

Once the site connection(s) is/are established, the Connection Tool launches the MOTOTRBO Connection Plus Network Manager. The Network Manager is the software application that is used to view and configure the connected XRC(s). A single instance of the Network Manager can manage simultaneous TCP/IP connections to multiple sites that share the same Network ID. This is known as the Connection Groups feature. However, only

one site a time can be selected for viewing and configuration. Because it is so easy to change the selected site when there are multiple sites in the Connection Group, it is important for the user to always be aware of which site is currently selected for viewing and configuration. The Site Number for the currently selected site appears at the bottom of the Network Manager screen.

XRT Gateway: The XRT Gateway is an optional component for the MOTOTRBO Connect Plus digital trunking system that allows certain 3rd party applications to interface with Connect Plus, supporting features such as a digital wireline console, automatic retrieval of airtime data, and providing an interface for some analog devices. If the XRT is used to initiate and receive calls, its impact on call loading and IP network bandwidth is similar to the impact of a Connect Plus site with 15 repeaters (30 timeslots). If the XRT client application is “streaming” Connect Plus airtime data, this uses additional IP bandwidth. For more information, see the sections on Connect Plus IP Network Bandwidth Considerations.

4 Connect Plus System Design Considerations

4.1 Migrating to Connect Plus from other MOTOTRBO Digital Modes

Migrating to Connect Plus from other MOTOTRBO Digital Modes involves several prerequisites and considerations:

- Each MOTOTRBO subscriber radio must have a Connect Plus Option Board, or a “Generic Option Board” that can be converted to Connect Plus operation through the installation of Connect Plus firmware. This must occur before the SU can be used for Connect Plus.
- Each MOTOTRBO subscriber radio must be enabled for the Connect Plus purchasable feature.
- Each MOTOTRBO subscriber radio must be configured for Connect Plus operation, both with MOTOTRBO CPS and with Connect Plus CPS.
- Connect Plus does not use Control Station Radios as the air interface for Location Tracking Applications or Text Message Applications. If these radios are no longer needed as a Control Stations for other MOTOTRBO modes, they can be used as Connect Plus mobiles.
- If desired, the non-Connect Plus zones and channels in the SU can be preserved, but they must be shifted in order so that they do not precede any Connect Plus zone. Guidelines for this procedure are provided in this document.
- In most cases, the Radio ID used in the previous MOTOTRBO Digital Mode can also be used in Connect Plus. There are two exceptions:
    - If the same Radio ID is used in more than subscriber unit, it must be changed to a different Radio ID that is not assigned to any other SU.
    - Radio ID’s 16776352 through 16776415 are not allowable for Connect Plus operation. If the radio’s current Radio ID falls into this range, it must be changed to an unused Radio ID in the allowable Connect Plus range. (1 to 16776351)
- The MOTOTRBO Repeater used in the previous digital mode can be used for Connect Plus operation, provided the following conditions have been met:

  - The repeater's software version must be capable of Connect Plus operation.
  - Both repeater timeslots will be used for Connect Plus.
  - The repeater will have to be re-configured with MOTOTRBO CPS in order to set several key parameters as required by Connect Plus.
  - The repeater will have to be connected via IP to a Connect Plus XRC Controller. The repeater must be in the same physical location as the XRC controller, and must be attached to the same Ethernet switch.

- The repeater frequency used in the previous MOTOTRBO digital mode can likely be used for Connect Plus. For more information, see Connect Plus Frequency Licensing Considerations.

Once the prerequisite conditions are met, the system can be migrated to Connect Plus operation.

Because the radios can be programmed with both Connect Plus and non-Connect Plus modes, the System Administrator has a couple of migration strategies to choose from:

- Talk Groups and Repeaters can be switched over to Connect Plus in a phased approach, with some Groups and Repeaters being switched to Connect Plus prior to others.

- The entire system can be switched over to Connect Plus at a specific time and date. Prior to the switch-over, all subscriber units must be enabled and programmed for Connect Plus operation.

Regardless of which strategy is chosen, this will have to be communicated to radio users. Each user should be instructed in how to switch the radio to Connect Plus operation (by selecting the Connect Plus zone and channel). Also prior to the switch-over, each user should be trained in how the radio operates in Connect Plus mode.

4.2 Connect Plus Frequency Licensing Considerations

4.2.1 Acquiring Frequencies

Frequency Licensing considerations and procedures for Connect Plus are similar to other MOTOTRBO digital modes. The reader can refer the section on Acquiring New Frequencies of [1]. Connect Plus has one additional (and essential) licensing consideration that does not apply to other MOTOTRBO digital modes.

In Connect Plus the downlink of the Control Channel timeslot transmits continuously. This minimizes the time the SU spends searching for service, and it allows the system to quickly respond to registrations and call requests. Any interruption to this continuous messaging adversely affects system performance. Because of this requirement, Connect Plus Control Channel frequency pairs require a Protected Service Area. Non-exclusive licenses such as FB2 or FB6 are not suitable for Connect Plus Control Channel operation (for more information refer to the "Licensing of Part 90 Radio Services" section).

4.2.2 Repeater Base Station Identification (BSI) for Connect Plus

The System Administrator should be familiar with the FCC station identification requirements for each licensed frequency. Station Identification is sometimes called "Base Station Identification" (BSI), and other times it is referred to as Continuous Wave Identification (CWID). The latter name is because "CW" is another name for Morse Code, which is used to send the station's call sign in analog BSI mode. In this document, BSI and CWID are used interchangeably.

Connect Plus enables the license holder to comply with ID requirements by providing a programmable BSI string and interval for each Connect Plus repeater. In other digital modes, BSI is handled entirely by the repeater. In Connect Plus mode, BSI is handled jointly by the repeater and the XRC controller. The identification string itself (usually the FCC license call sign) is programmed into the repeater with MOTOTRBO CPS, but the TX Interval is programmed into the XRC Controller with the MOTOTRBO Connect Plus Network Manager. It is important to program the repeater's BSI string with MOTOTRBO CPS prior to programming the Interval on the Network Manager's BSI Schedule. In Connect Plus mode of operation, the repeater knows to ignore the BSI TX Interval programmed with MOTOTRBO CPS. The Controller will tell the repeater when to send BSI. If the repeater "NACKs" the controller's request for BSI, the operation depends on the NACK reason. If the NACK indicates that the repeater has not been programmed with a BSI, the XRC will automatically change the BSI interval for that repeater to zero (indicating no BSI). The BSI interval will remain at zero until the radio system administrator changes it to a different value with the Network Manager.

Configure the repeater's BSI settings with MOTOTRBO CPS prior to configuring the Interval with the Network Manager. If BSI cannot be sent at the present time for some other reason, the controller restarts the BSI Interval timer for that repeater. When the interval elapses, the controller will send the BSI request again. Whenever the controller cancels a BSI session due to repeater NACK(s), it places a time-stamped "BSI Error" (or "Digital BSI Error") into its Event Log, which can be retrieved and viewed with the Network Manager. The BSI Error indicates the repeater's Radio ID, and states whether the controller will reschedule the BSI. The Digital BSI Error indicates the repeater's Radio ID, targeted BSI timeslot and failure reason.

Beginning with MOTOTRBO System Release 1.7 (R2.6.0), repeaters with supporting firmware can be configured to send either Analog BSI or Digital BSI, depending on the BSI Mode configuration of the repeater channel personality. Digital BSI sends the license identification string via digital text message rather than via analog CWID (Morse Code). Prior to enabling Digital BSI on a repeater, the system administrator (or owner) should check to see if Digital BSI is permitted by the repeater's frequency license.

Wherever it can be used, Digital BSI provides some advantages over analog BSI:

- Digital BSI can be sent over a single digital timeslot and does not interrupt calls or signaling on the other timeslot. Therefore, Digital BSI can be sent on slot 2 of the Control Channel repeater without interrupting control signaling on slot 1. With Digital BSI, it is also possible to send BSI on repeaters with a Fast GPS Channel or prolonged file transfer, provided that both slots are not in use for those types of sessions. When the repeater is enabled for Digital BSI, the controller automatically picks the best timeslot to use.

- Because Digital BSI is sent via text message, it can be transmitted more quickly than Analog BSI which is sent via Morse Code.

Whenever possible, analog BSI should be sent on trunk channel repeaters only. Analog BSI on the Control Channel repeater interrupts Control Channel messaging, and will cause significant operational problems to radios using the site – it should be avoided if at all possible. During analog BSI the repeater transitions to analog mode and ceases all digital signaling. During Control Channel analog BSI, the SU cannot register or request calls, and the Control Channel cannot send messages for calls in-progress. Prior to starting analog BSI on the Control Channel repeater, the controller sends a special message on the Control Channel downlink. Any SU that decodes this message will start a configurable timer called "BSI Wait Time" (configured with MOTOTRBO Connect Plus Option Board CPS). The value programmed for this timer must allow enough time for the repeater to send the analog BSI and for the Control Channel messaging to resume. SUs that decode the special message will not move to other sites during analog BSI (provided their timer doesn't expire), but they will display "Searching" until the analog BSI finishes and the Control Channel messaging returns. SUs that do not decode this special message will attempt to locate another site during analog BSI.

4.2.3 Licensing of Part 90 Radio Services

Based on the Federal Communications Commission (FCC) rules and regulations[40] in the United States, trunking radio service can be on shared channels or exclusive channels. To determine the type of license needed, please consider the following:

- IG = Business/Industrial, Conventional
- YG = Business/Industrial, Trunking (**Connect Plus**)
- FB2 = Repeater on shared channel, internal systems
- FB6 = Repeater on shared channel, for profit systems
- FB8 = Repeater on exclusive channel

In the **700/800/900 MHz** bands, the channels are paired and normally licensed as exclusive.

In the **UHF** band, the channels are paired and normally licensed as shared. It requires additional coordination effort to find and license exclusive channels.

In the **VHF** band, the channels are **not** paired – base/mobile simplex channels – and are normally licensed as shared. It requires additional coordination effort to find and license shared repeater channel, and then the additional coordination effort to license repeater channels as exclusive.

Trunked systems, like Connect Plus, are often high traffic systems with a dedicated, continuous Control Channel and are usually licensed on exclusive channels. Continuous Control Channel must be exclusive (FB8), but traffic channels could be either exclusive (FB8) or shared (FB2/FB6). If the traffic channels are expected to have a high activity level, they should be exclusive (FB8). Shared traffic channels (FB2/FB6) must be capable of monitoring channel before transmitting, which usually means lower channel traffic levels.

There are two levels of monitoring for shared channels:

- **Level I** – Repeater monitors base receive channel for mobile activity (normal channel monitoring). The RSSI threshold setting in MOTOTRBO repeaters is used for FCC Type 1 compliance, as it is used to measure the maximum interference signal that the MOTOTRBO repeater tolerates. The challenge with Level I monitoring is that there could be a 'hidden node' issue where distant foreign subscribers may not be heard. Same issue occurs on normal conventional repeater channels.
- **Level II** – Requires separate remotely located monitor receiver on the repeater transmit frequency to listen to co-channel repeater output channel. This eliminates the 'hidden node' issue and is recommended if there is interference between systems using Level I monitoring.

Note: The above guidelines apply to part 90 services. Auction channels are still available in Part 22 and Part 80 in the US.

4.3 Digital Channel Loading for Connect Plus

Accounting for repeater loading is a critical step in designing a Connect Plus system. Such planning ensures that the designer is able to choose the number of channels required to support the customer’s typical communication needs at the expected level of service. The first step is to estimate how much traffic a single slot (channel) can support. An important distinction in Connect Plus is the fact that it is digital trunking system, which means that the loading estimation models will be different than the other digital modes supported by MOTOTRBO. Since the traffic, consisting of voice, text messages, location updates, and registration requests, is mostly initiated by the end user, it is challenging to predict how often it occurs. Standard usage profiles of existing customers have been created for voice and data services. These profiles act as a baseline for estimating how much traffic a user

[40] Part 90 – Private and Land Mobile Radio Services

creates on a system. If the standard profiles do not match your customer's expected usage, further estimations based on the trend lines need to be considered. After the system is used, and real life usage is identified, further adjustments may be required.

4.3.1 Voice and Data Traffic Profiles

The following table outlines the typical user traffic that is based on empirical data. These usage profiles are considered standard and are utilized to estimate the number of users that can be supported per channel. These estimates are depicted on graphs in the in the sections that follow. The same user traffic assumptions have been used for other non-Connect Plus digital configurations as well. The reader can refer to Digital Repeater Loading section in [1] for more details.

Profile Name	Traffic Type	Call Description	Traffic Per User Per Hour	
High Voice	Group Voice Call	10 second call, 2 transmissions per call	3.0 Calls per User per Hour	90%
	Individual Voice Call	20 second call, 4 transmissions per call		10%
Low Voice	Group Voice Call	10 second call, 2 transmissions per call	1.0 Calls per User per Hour	90%
	Individual Voice Call	20 second call, 4 transmissions per call		10%
High GPS	Location Updates	2 seconds per transmission	60 GPS Transmissions per User per Hour i.e. 1 Minute Update Period (Cadence)	
Low GPS	Location Updates	2 seconds per transmission	6 GPS Transmissions per User per Hour i.e. 10 Minute Update Period (Cadence)	
High Text Messaging	Text Messaging	100 characters per message	2.5 Text Messages per User per Hour	
Low Text Messaging	Text Messaging	100 characters per message	0.5 Text Messages per User per Hour	

Table 4-1 Voice and Data Traffic Profiles

4.3.2 Estimating Loading For Connect Plus

The following charts in Figure 4-1 and Figure 4-3 represent loading characteristics of a Connect Plus system based on a certain user experience, for a given number of active (call participants) users, and for different combinations of Voice and Data Profiles as defined in 4.3.1.

The charts represent a radio user's experience in making a call in terms of Grade of Service (GoS). GoS is directly related to the probability of a call getting blocked i.e. probability of all the trunked channels being busy. For example, a GoS of 2% means that 2% of the calls made by the radio users will need to wait in the Busy Queue for a channel to become available.

The “channel” in the chart refers to a logical channel (i.e. a timeslot). In Connect Plus, both channels of a repeater are in trunked mode (except for the Control Channel repeater). Therefore, the charts provide the number of users only for an even number of channels.
The number of calls handled by a Connect Plus system may vary considerably based upon the number of users and volume of calls. Typical systems are heavily loaded for a few hours in a day. It is recommended that the system be designed with an adequate amount of channel resources to handle both peak and off-peak traffic. The charts in this section represent estimated number of active users that can be supported **per site**.
The call profiles below assume that GPS location updates are sent via the non-Fast GPS method, which utilizes shared traffic channels for voice and data calls. Channel capacity and throughput for dedicated Fast GPS Report Channels is described in the section titled "*Connect Plus Fast GPS*".

The first chart (Figure 4-1) is for High Voice profile (i.e. 3 Calls per User per Hour) with no GPS data, whereas Figure 4-2 illustrates the capacity for Low Voice (i.e. 1 Call per User per Hour) with no GPS traffic.

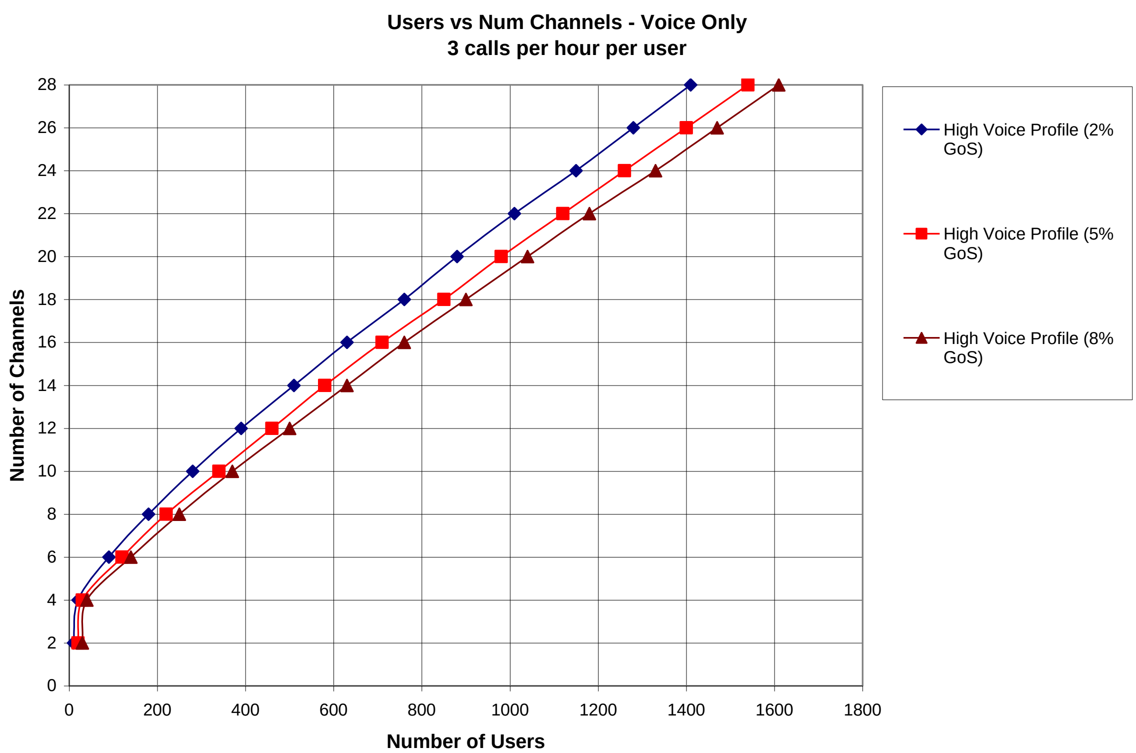


Figure 4-1 Users vs. Number of Channels for High Voice-Only Traffic

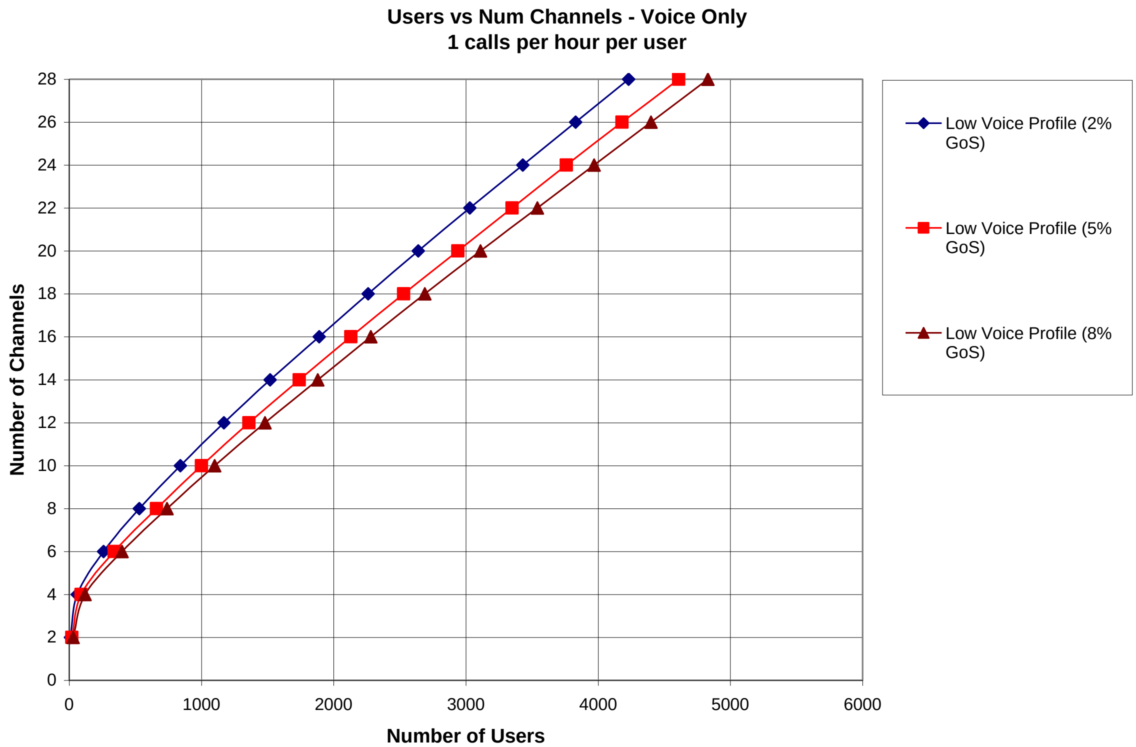


Figure 4-2 Users vs. Number of Channels for Low Voice-Only Traffic

Figure 4-3 is for mixed voice and GPS data profile. The graph shows High Voice with low GPS data traffic. Since Connect Plus is a trunking system, both voice and GPS data are using the trunked channels. The reader should note the trend indicated in the chart – the number of users does not increase proportionally with the number of channels. The rate increases as the number of channels increase. This is due to the fact that the efficiency of trunking increases with the increase in the number of channels.

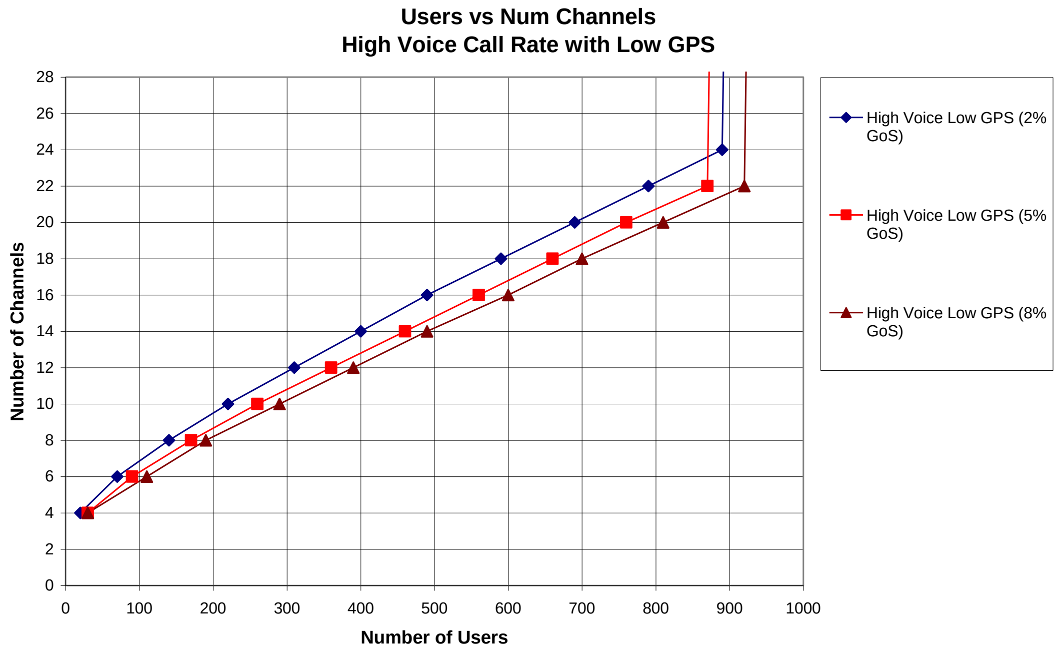


Figure 4-3 Users vs. Number of Channels for High Voice & Low GPS Traffic

Figure 4-4 depicts the loading profile for Low Voice call rate with Low GPS updates.

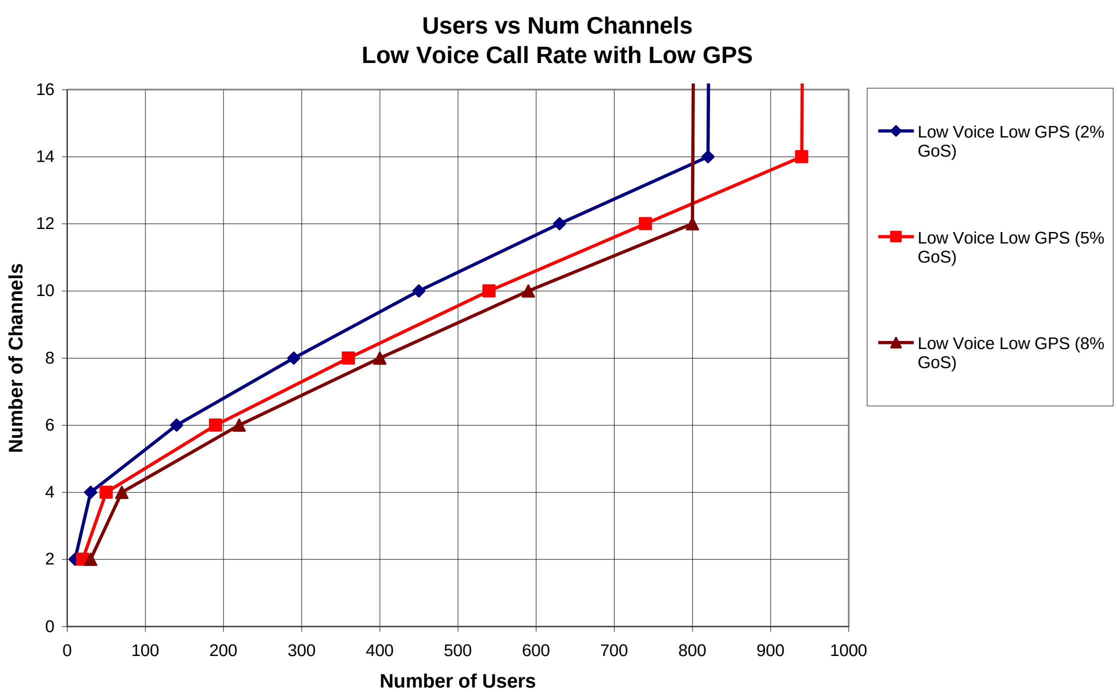


Figure 4-4 Users vs. Number of Channels for Low Voice & Low GPS Traffic

In the case of high GPS data, it is recommended that a Connect Plus system have sufficient trunked channel allocated for Location Updates. The *Number of Data Sessions Allowed* parameter in the XRC controller can be set to a higher value to accommodate this type of traffic.

When a Connect Plus site services both voice calls and data calls – such as text messaging and Generic/Packet data – initiated by the subscribers, it is important to note that the total **data call rate** from all radios should not exceed 2 calls per second. This is due to the voice-centric system design, which gives preference to the voice calls and thus reserves smaller amount of bandwidth on the control channel to grant data call requests. Overall, the data call rate that can be serviced by the system is determined by factors such as current site activity and the number of RF resources.

4.3.3 Setting Repeater Hang Times in Connect Plus

When Connect Plus radios move to a trunk-to timeslot to participate in a voice call, the Call Hang Time allows an opportunity for talk-back using the same Call ID, without having to return to the Control Channel to request a new call. Besides providing an opportunity for talk-back on the assigned timeslot, the Call Hang Time helps provide continuity to the conversation and prevents the channel from being assigned to another call. The Call Hang Time is configurable per call type for “Group Call”, “Private Call”, and “Emergency Call”.

In other digital modes, the repeater can be configured with a “zero” Call Hang Time to create a “transmission trunking” environment where each PTT is treated as a brand new call. This configuration is not recommended or supported in Connect Plus because the time required for Control Channel call processing, validation, channel assignment, and synchronization with the assigned timeslot would have to be repeated for each PTT.

Selecting value(s) for the Call Hang Times is one of the most important decisions to be made when configuring a system. There are pluses and minuses to both “longer” and “shorter” Hang Time values. Selecting the best Call Hang Time value is somewhat of a trade-off, and will vary according to the needs of the system and its users.

Longer Hang Time values provide the greatest opportunity for the radio user to talk-back on the assigned channel without having to start a brand new call. This benefits both the user and the system. Speaking during the Hang Time of an existing call provides faster access than having to start a new call. It also assures that the speaker will have an available channel, whereas a new Call Request might be placed in the Busy Queue. Longer Hang Time values also help reduce Control Channel congestion on busy systems. On the other hand, longer Hang Time values are perceived as detrimental when the call is really over and users must wait for the channel to drop.

It should be noted that Connect Plus does not recommend or support a value of “zero” for Call Hang Times. The default Call Hang Time Values (3 seconds for Group Call and 4 seconds for Private and Emergency Calls) or longer are recommended. In many systems Private Call Hang Time is set longer than the Group Call Hang Time (due to the additional call set-up messages before a Private Call), and Emergency Call Hang Time is set longer than either Group Call or Private Call. See section “Programming the Repeater’s Emergency Call Hang Time” for important considerations for setting the Emergency Call Hang Time.

The Connect Plus Network Manager has configurable settings for “Group Call Hang Time”, “Private Call Hang Time” and “Emergency Call Hang Time”. The XRC uses these values to automatically configure the repeater’s Call Hang Timers during Link Establishment. The repeater uses the Network Manager values as long as it maintains connectivity to the XRC, but it does not save the Network Manager-configured values to persistent memory. If MOTOTRBO CPS is used to read the repeater’s codeplug, it will display the CPS-configured values, not those set with the Network Manager. If the repeater loses connectivity with the XRC and enters conventional fallback mode, it uses its CPS configured Hang Time values. When the XRC comes back on line, the repeater will automatically initiate Link Establishment with the controller. If Link Establishment is successful, the repeater will exit conventional fallback operation, and will once again use the Hang Time values that were configured with the Network Manager.

The radio System Administrator must assure that the value chosen for each Call Hang Time setting is programmed the same into each Connect Plus repeater and site network-wide. The XRC helps with this requirement by automatically configuring each of the site's repeaters with the Hang Time values programmed with the Network Manager. However, the System Administrator must assure that all XRC controllers in the multisite network are configured with the same Hang Time values.

4.4 Multiple Digital Repeaters in Connect Plus Mode

4.4.1 Configuring Connect Plus Repeaters with MOTOTRBO CPS

The MOTOTRBO repeater is a required component of the Connect Plus trunking system, as it provides the RF path between the Connect Plus Controller and the Connect Plus SU.
Each XRC Controller can control up to 15 MOTOTRBO repeaters. The XRC and its connected repeaters must be in the same physical location, and connected to the same Ethernet switch. The XRC acts as the Link Establishment (LE) Master and the connected repeaters are configured as LE Peers. Beginning with MOTOTRBO repeater release R2.3, the repeater must be configured to operate exclusively in Connect Plus mode using the MOTOTRBO CPS – the "System Controller Mode" must be enabled in the repeater codeplug.

Before the MOTOTRBO Repeater can operate in a Connect Plus system, it must be configured with MOTOTRBO CPS according to the guidelines provided below. These guidelines do not address every programmable repeater parameter, just the settings that are critical to Connect Plus operation.

Prior to configuring the repeater, use MOTOTRBO CPS to read the repeater's codeplug. Then, from the MOTOTRBO CPS Main Menu select "View", and then select "Expert" from the drop-down View Menu. This will assure that the programmer sees all of the settings discussed in the tables below.

MOTOTRBO CPS General Settings screen
Settings critical to Connect Plus Operation

Setting	**Notes and Additional Information**
Radio ID	Each Repeater must be programmed with a unique Radio ID (1-15). Once a Radio ID is used, it cannot be repeated in the same Connect Plus site. However, because Connect Plus restricts all repeater Radio ID's to the same 15 numbers, they can be re-used at different sites. The Radio ID must match the frequency configuration for this repeater & site in the Connect Plus Network Frequency File.
SIT (Subscriber Inactivity Time)	The SIT value configured into the repeater with MOTOTRBO CPS will be overwritten by the XRC during Link Establishment with the repeater. The XRC will set the repeater's SIT based on the Call Hang Time values configured with the Connect Plus Network Manager. The repeater will use the SIT value sent by the XRC as long as it maintains its connection to the XRC.
Group Call Hang Time	The Group Call Hang Time must be configured with the same value for all Connect Plus repeaters and sites in the same network. The Group Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Group Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See section "Setting Repeater Hang Times in Connect Plus" for important information on selecting the Group Call Hang Time value.
Private Call Hang Time	The Private Call Hang Time must be configured with the same value for all Connect Plus repeaters and sites in the same network. The Private Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Private Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See section "Setting Repeater Hang Times in Connect Plus" for important information on selecting the Private Call Hang Time value.
Emergency Call Hang Time	The Emergency Call Hang Time must be configured with the same value for all Connect Plus repeaters and sites in the same network. The Emergency Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Emergency Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See section "Setting Repeater Hang Times in Connect Plus" and section "Programming the Repeater's Emergency Call Hang Time" for important information on selecting the Emergency Call Hang Time value.
CWID	If this repeater must send CWID to satisfy FCC requirements, enter the ID in this field. In Connect Plus trunking operation, the repeater will ignore the TX Interval programmed with MOTOTRBO CPS. The TX interval for this repeater must be set in the XRC controller (using the Connect Plus Network Manager). For Connect Plus Auto Fallback operation, the repeater uses the interval programmed with MOTOTRBO CPS.
TX Power Settings	Repeater Power Settings should be set the same for all repeaters in the same site. This is because all repeaters in the same site must have the same coverage footprint.

Privacy Type	If this repeater site will be used by any subscriber radio enabled for Enhanced Privacy, then set the Privacy Type to “Enhanced”. If not, then set the Privacy Type to “None”. (Connect Plus does not support the “Basic” Privacy Type.)

MOTOTRBO CPS Network screen and Link Establishment Screen
Settings critical to Connect Plus Operation
Note: Depending on the repeater firmware and MOTOTRBO CPS software version, the settings may not appear in the same order as listed below and the setting names may be slightly different. The Network Settings and Link Establishment settings may appear on the same screen, or on separate screens.

Setting	Notes and Additional Information
CAI Network	Set to 12 (default setting)
CAI Group Network	Set to 225 (default setting)
Link Establishment Link Type	Set to “Peer”
Master IP	Enter the IP Address of the XRC Controller
Master UDP Port	Each repeater in the site must be programmed with a unique number for “Master UDP Port”. The number must fall between “First UDP Repeater Listen Report” (a programmable controller parameter) and “First Repeater Listen Port” +14
Ethernet IP	If DHCP is not used, enter the repeater’s Ethernet IP in this field. This must be a unique IP address that is not used for any other device at this, or other sites.
IP Site Connect Beacon Duration	Set to “Disabled”
IP Repeater Programming Enable	This box is only displayed for 32MB repeaters. Check the box to allow the repeater to be remotely programmed (via IP) with an authorized version of MOTOTRBO CPS. This is a purchasable feature for MOTOTRBO CPS.

MOTOTRBO Channel Screen
Settings critical to Connect Plus Operation

Setting	Notes and Additional Information
Color Code	Color Code must match the information for this Radio ID and frequency pair (for this site) in the Network Frequency File.
System Controller Mode	Must be enabled (checked). This option is available starting with MOTOTRBO repeater version R2.3. The repeater cannot be used as a Connect Plus resource until System Controller Mode is enabled.
IP Site Connect	Must be set to None for MOTOTRBO repeater version R2.3 or newer. Must be set to “Slot 1 & Slot 2” for legacy repeaters.
Messaging Delay	In conventional IP Site Connect, this sets the repeater’s arbitration timer. In Connect Plus, arbitration is done by the XRC controller, which has a programmable parameter called “Arbitration Time”. When the repeater is programmed for Connect Plus, leave the Messaging Delay at the default setting of “Normal”.
RSSI Threshold	This threshold is used to measure the maximum interference signal that the repeater will tolerate. If the repeater detects an interfering signal at or above this threshold, it takes itself offline and reports its off-line condition to the XRC Controller. If the Control Channel repeater were to take itself off-line, site operations would be severely impacted. For this reason the interference threshold for the Control Channel repeater should be set quite high (in the range of -80 to -40 dBm). Connect Plus Control Channel frequency pairs require a Protected Service Area. Non-exclusive licenses such as FB2 or FB6 are not suitable for Connect Plus Control Channel operation.
RX Frequency & TX Frequency	Repeater frequencies must be different for each repeater in the site. The frequency information must match the information for this Radio ID and frequency pair (for this site) in the Network Frequency File.
Power Level	Should be set the same for all repeaters in the same site. This is because all repeaters in the same site must have the same coverage footprint.
TOT (Time out Timer)	Must not be set any shorter than the longest TOT in any transmitting device. The “transmitting device” can be a Connect Plus SU, or a non-radio device (such as a wireline console connected through the XRC, etc).

Note: Other channel settings may be displayed, depending on device features, hardware, and repeater firmware level. If Phone Gateway setting is displayed, set to “None” for Connect Plus operation. If “IF Filter Type” setting is displayed, refer to MOTOTRBO CPS Help for information. If “BSI Mode” setting is displayed, set to Analog or Digital. See section “*Repeater Base Station Identification (BSI) for Connect Plus*” for more information.

4.4.2 Coverage Area of Connect Plus Repeaters in Single-Site Configuration

Trunking is based on the assumption that the SU can communicate with every site repeater just as well as it communicates with the Control Channel repeater. For this reason, all repeaters under the control of the same XRC controller must reside in the same RF frequency band and must all have an identical coverage footprint (both “talk in” and “talk out”).

4.4.3 Frequencies and Color Codes in a Connect Plus Single Site System

Because all of the MOTOTRBO repeaters in the same Connect Plus site have the same coverage footprint, they must be programmed with different frequencies, so as not to interfere with one another. Figure 4-5 shows an example of a Connect Plus Single Site system. All of these frequencies must be in the same RF frequency band. For example, if any site repeater is in the VHF band, then all site repeaters must be VHF also. The Color Codes can be the same, or they can be different.

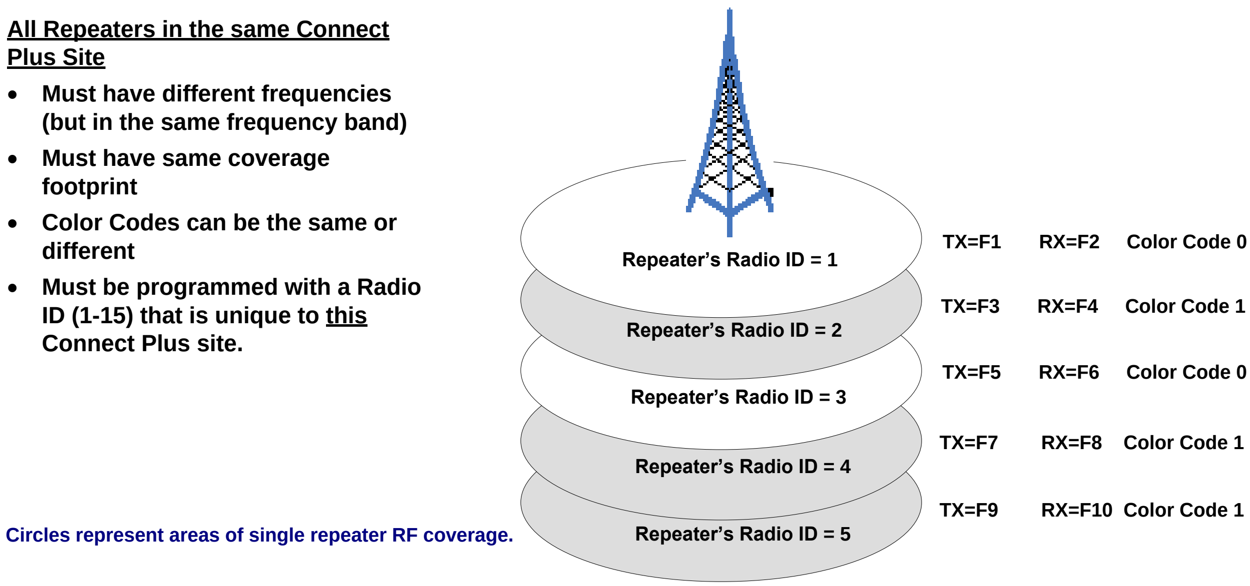


Figure 4-5 Multiple Digital Repeaters in Connect Plus Single Site

The following information for each repeater in the Connect Plus network must be programmed into the SU's Network Frequency File:

- Which site the repeater is located at.
- The repeater's Radio ID (1-15). In the Connect Plus system, this equates to the channel (repeater) number.
- SU TX (Repeater RX) Frequency
- SU RX (Repeater TX) Frequency
- The repeater's Color Code
- A checkbox to indicate if the repeater is the Control Channel Frequency. Up to four repeaters per site can be checked as Connect Plus Control Channels. (Only one repeater at a time will be the active Control Channel repeater.) The Control Channel information in the Network Frequency file must match the list of Control Channel repeaters configured into the site's XRC Controller with the Connect Plus Network Manager.

For proper operation, the Network Frequency File must match the actual network configuration at all times. If changes are made to any of the information listed above, it will be necessary to provide the SU with an updated version of the Network Frequency File. For more information on the Network Frequency File, and the options for providing the SU with an updated file, see "Network Frequency File" in the System Feature Overview Section.

4.4.4 Coverage Area of Connect Plus Repeaters in Multisite Configuration

The most common reason for connecting multiple sites is to enlarge the RF coverage available to the Connect Plus SU. Because of this, each Connect Plus site is typically placed in a different geographical area and provides the RF coverage for that area. As the radio user moves from one coverage area to another, the SU is able to automatically "Roam" from one site to another.

When there are multiple Connect Plus sites, the ideal topology is for the RF coverage of each Connect Plus site to over-lap slightly with its geographically adjacent neighbor sites. This emulates the "cellular" network design where each site is a "cell" in a network of slightly overlapping cells. This design will provide the most satisfactory operation for automatic Roaming by the Connect Plus SU.

It's possible that circumstances beyond the control of the network designer will necessitate a departure from the ideal topology of slightly overlapping coverage cells. Examples include the following:

- Rather than providing "slightly overlapping coverage" in all cases, some sites have no overlapping coverage at all. They are separated from other sites by "dead areas", where there is no coverage at all.
- Rather than providing "slightly overlapping coverage" in all cases, the coverage areas of some sites may overlap significantly.
- Some networks may have combinations of different coverage characteristics; slightly overlapping for some sites, no overlap for some sites, significantly overlapping for some sites.

Topologies such as these provide greater challenges when configuring the Roam parameters of the Connect Plus SU. For mixed topologies, the Roam settings will be a compromise that provides acceptable (though probably not optimal) Roam operation by the Connect Plus SU. For a detailed discussion on Connect Plus Roaming (also called "Site Search), see the System Feature Overview Section.

4.4.5 Frequencies and Color Codes in a Connect Plus Multisite System

Because the most common reason for connecting multiple sites is to enlarge the RF coverage available to the Connect Plus SU, all of the frequencies in a multisite network are typically in the same RF frequency band. Because a single SU operates in just one frequency band, this makes the entire network coverage area accessible to the SU.

A less common reason for linking multiple Connect Plus sites is to provide communications between MOTOTRBO radios that use different frequency bands. In this case, each frequency band requires its own Connect Plus site(s), and each SU will only be able to access the site(s) within its own frequency band.

While the repeaters in any single Connect Plus site must all use different frequency pairs, frequencies may be re-used at different sites when coverage does not overlap. If coverage does not typically overlap, but may in certain conditions (such as when the SU is in a very high place), the re-used frequencies must have different Color Codes. This will not eliminate interference between the two repeaters, but it will help SU's distinguish between the different repeaters – especially while Roaming.

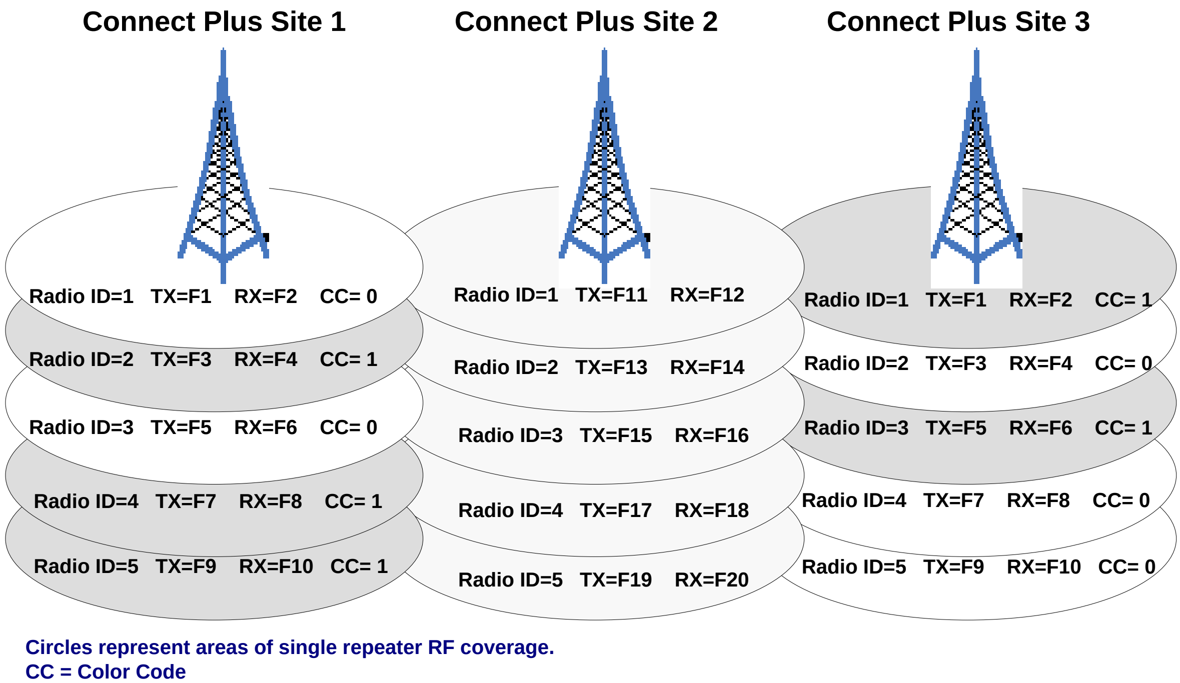


Figure 4-6 Multiple Digital Repeaters in a Connect Plus Multisite System

As stated previously, the Network Frequency File must match the actual network configuration at all times. If changes are made to any of the information listed above, it will be necessary to provide the SU with an updated version of the Network Frequency File. For more information on the Network Frequency File, and the options for providing the SU with an updated file, see " *Network Frequency File"* in section "Connect Plus System Feature Overview".

4.5 Considerations for the Connect Plus Backend Network

The reader is strongly encouraged to review the section on *Consideration for the Backend Network* related to IP Site Connect digital mode outlined in [1].

The first characteristic of a backend network required for adequate Connect Plus operations is broadband connectivity with relatively low delay; Connect Plus cannot operate over a dial-up connection or satellite link (due to high delay).

The XRC controller is the master device at the site and it communicates with the collocated repeaters over UDP/IPv4. The XRC communicates with other site controllers over both UDP/IPv4 and TCP/IPv4 depending on the traffic type. The controller requires a static IP address whereas the repeaters may utilize a DHCP server to acquire an IP address on power up. The dynamic address of a repeater is selected by selecting the DHCP option in the repeater CPS. It is recommended that the lease time of the IPv4 address from the DHCP should be kept as long as possible to minimize the frequency of possible short service disruptions upon IPv4 address renewal. A Connect Plus repeater registers its IPv4 address with the controller during power-on and upon a change in its IPv4 address. The controller maintains a table of IPv4 addresses and port numbers of its collocated repeaters. Furthermore, in a multisite Connect Plus configuration, the controller keeps a table of IPv4 addresses assigned to the controllers located at the other sites to be able to facilitate registration requests, facilitate inter-site call setup, and forward user voice and data traffic to targets registered in different sites.

The Connect Plus devices may be installed behind a network firewall. In such case, for successful communication between controllers at different sites, the firewall (router) has to be programmed to forward the Connect Plus

inter-site traffic to a pre-defined set of TCP and UDP ports. The reader can refer to [4] to learn the step for configuring the XRC Controller for multisite operations.

Important Note: The XRC, XRT, and XRI do not currently support multicast IP traffic. The System Administrator must design or configure the IP network such a way that no Multicast messages are sent to the XRC, XRT or XRI.

4.5.1 Characteristics of Backend Network

Besides the requirement for broadband network rates, there are other IP network characteristics that are necessary to meet the customer expectations for clear voice communications, low delay and reliable data calls. These are briefly described below:

1. **Delay (Latency)** – Network delay for a two-way radio system is defined as time for voice to leave the source repeater and reach the destination repeater. Furthermore, the overall delay is comprised of the following components:
    a. **Propagation delay** – caused by the distance an electrical signal must travel on the physical medium of the backend network, such as copper wire, fiber link or backhaul microwave connection.
    b. **Serialization delay** – represents the amount of time necessary for the source repeater to actually place a packet byte by byte on its network interface.
    c. **Handling delay** – defines the aggregate delay incurred by the intermediary devices that forward a packet through the backend network. Examples of such devices are the XRC Controller, switches and routers which introduce queuing delays when more packets are transmitted to a network device than the device can handle.

    The network delay should be considered when setting the programmable “Arbitration Time” setting in the XRC controller. Upon receiving IP voice packets, the controller waits the arbitration time prior to forwarding the voice packets to the repeater for transmission. In the event of near-simultaneous key-ups at different sites during the same call, arbitration increases the chances that the same audio will be heard at all sites involved in the call. It is strongly recommended that the Connect Plus system **not** be installed on an IP network inducing a delay higher than 180 ms, although for optimal performance the delay should not exceed 60 ms (see also “Packet Loss” description below).

2. **Jitter** – Jitter is defined as variation of network delay. The source device is expected to transmit packets at regular interval, which accounts for a network delay as explained above. However, due to inconsistent queuing delays these packets may not arrive at the same interval. Such variation constitutes Jitter. Connect Plus implements a jitter buffer of 60 milliseconds to handle such effects. Any jitter above such levels significantly affects the audio quality.

3. **Packet Loss** – Packet loss in IP-based networks is both common and expected. To transport voice bursts in timely manner, Connect Plus utilizes UDP/IPv4, which is not a reliable transport mechanism (e.g. confirmed delivery). Therefore, while designing and selecting the backend network it is necessary to keep packet loss to a minimum. The Connect Plus system responds to periodic packet loss by replaying either a special packet (in the case of voice) or the last received packet (in the case of data). In the case of voice, the ongoing call ends if six consecutive packets do not arrive within 60 ms of their expected arrival time. In the case of data, the repeater waits for the expected number of packets (as per the data header) before ending the call.

4.5.2 Connect Plus IP Network Bandwidth Considerations

Bandwidth is the rate of data transferred to and from a network device, often referred to as the bit rate. Bandwidth is measured in bits per second (*bps*) or kilobits per second (*kbps*). When designing a Connect Plus system, it is important to understand the needs of each Connect Plus device, so that the appropriately rated network connection for each site can be chosen.

If a customer has high speed network connections between sites, these calculations may not be as important, but if they are working on lower speed public Internet Service Providers (ISPs) it is good practice to understand these values and plan accordingly. If the minimum amount of bandwidth is not available, the end user may experience audio holes or even dropped calls. Data messaging or RDAC commands may not be successful on the first attempt, or may be dropped all together. In general, the quality of service may suffer if substantial bandwidth is not available.

Note that for most Internet Service Providers, offer asymmetric broadband channel, such that the uplink bandwidth is lower than the downlink. The downlink bandwidth is usually multiple factors above the uplink bandwidth. Therefore, it is important to understand such differences and account for them when designing a backend network. Some ISPs may advertise a particular bandwidth, but it is important to verify the promised bandwidth is available once the system is installed and during operation.

It is also important to note that if the wide area network connection is shared with other services (file transfer, multimedia, web browsing, etc.), then the Connect Plus devices may not have the appropriate bandwidth when required and quality of service may suffer. It is recommended to remove or limit these types of activities. In addition, excessive usage of the RDAC application or the Network Manager's real-time monitoring features may cause increased strain on the network during times of High Voice activity.

4.5.3 Required Bandwidth Calculations (no VPN)

Meeting the bandwidth requirements for a single site Connect Plus may not be a challenging task, because the XRC Controller, the local repeaters and the computers hosting the applications will, most likely, be connected through a modem Ethernet switch, which can manage traffic that is far greater than even a fully loaded system can generate.

On the other hand, when designing a multisite system the administrator/dealer should carefully consider the amount of IP data traffic that will flow between the sites based on the number of repeaters, the network location of the machines hosting the user applications (text messaging, location) and those running the diagnostic and fault management tools (RDAC, Network Manager).

Moreover, Connect Plus requires bandwidth for performing maintenance tasks such as upgrading XRC/XRT/XRI firmware, backing up or restoring controller configuration and user registry, as well as downloading event and airtime logs. Such administrative activities should **not** be carried out on an active site servicing user calls, but during off-peak hours. In general, for Connect Plus multisite configuration, it is **strongly recommended** each site link to have at least a T1 (~1.5 Mbps) dedicated capacity, unless the formula discussed below dictates the need for higher bandwidth.

The following equation should be used to calculate the bandwidth requirements for a Connect Plus RF site and then added together for sites, which reside behind one wide area connection.

BW_{VC} = 15 kbps = Bandwidth required to support Multisite Voice or Data (1 slot)
BW_{MC} = 10 kbps = Bandwidth required to support Multisite control messaging
BW_{RD} = 55 kbps = Bandwidth required to support RDAC commands[41]
BW_{NM} = 55 kbps = Bandwidth required to support Network Manager real-time monitoring
BW_{XRT} = 55 kbps = Bandwidth required to support XRT airtime data streaming mode

[Number of Multisite sites where call on slot **1** is repeated] - 1	**X**	BW_{VC}	kbps =		kbps
[Number of Multisite sites where call on slot **2** is repeated] - 1	**X**	BW_{VC}	kbps =		kbps
…	**X**	BW_{VC}	kbps =		kbps
[Number of Multisite sites where call on slot **N** is repeated] - 1	**X**	BW_{VC}	kbps =		kbps
[Multisite control messaging for total number of sites] - 1	**X**	BW_{MC}	kbps =		kbps
Network Manager Traffic		BW_{NM}	kbps =		kbps
XRT Streaming Airtime Data Traffic		BW_{XRT}	kbps =		kbps
RDAC Traffic[42]		BW_{RD}	kbps =		kbps
			+		
Required Uplink/Downlink Bandwidth					kbps

Table 4-2 Bandwidth Calculation Matrix for RF Site

To illustrate the use of the above equation on a more complicated Connect Plus system configuration, see the following example system shown in the diagram below. This Multisite system has 3 repeaters per site with 6 sites total; one site has an RDAC and a Network Manager. The routers are not utilizing VPN. We assume all trunk-to timeslots are occupied with multisite calls. Although this is an **extreme example** (because usually not all local calls are routed to every Connect Plus remote site), it provides the system administrator with basic guidelines on bandwidth allocation needs.
Note that user data application such as text messaging and location services are excluded from this sample system. If these services are activated then more bandwidth may be warranted.
Using the formula shown in Table 4-2, the bandwidth calculations for Site 1 in Figure 4-7 are as follows:

[Number of Multisite sites where call on slot 1 is repeated] - 1	5	x	15	kbps =	***75***	kbps
[Number of Multisite sites where call on slot 2 is repeated] - 1	5	x	15	kbps =	***75***	kbps
[Number of Multisite sites where call on slot 3 is repeated] - 1	5	x	15	kbps =	***75***	kbps
[Number of Multisite sites where call on slot 4 is repeated] - 1	5	x	15	kbps =	***75***	kbps
[Number of Multisite sites where call on slot 5 is repeated] - 1	5	x	15	kbps =	***75***	kbps
[Multisite control messaging for total number of sites] - 1	5	x	10	kbps =	***50***	kbps
Network Manager Traffic[43]					***55***	kbps
XRT Streaming Airtime Data Traffic					***55***	kbps
RDAC Traffic[44]					***0***	kbps
				+		
Required Uplink/Downlink Bandwidth for Site 1					***535***	kbps

Table 4-3 Example of Bandwidth Calculations for Connect Plus RF Site

[41] When the RDAC instance resides behind a firewall with NAT the RDAC bandwidth requirements should be omitted from the calculation since RDAC application must be on the same Local Area Network (LAN) or Virtual Private Network (VPN) as the controller and the site's repeaters.
[42] The RDAC calculation should be omitted if the hosting PC is behind a NAT router.
[43] Data traffic generated by the Network Manager located at Site 3, as shown.
[44] No RDAC at Site 1 as shown.

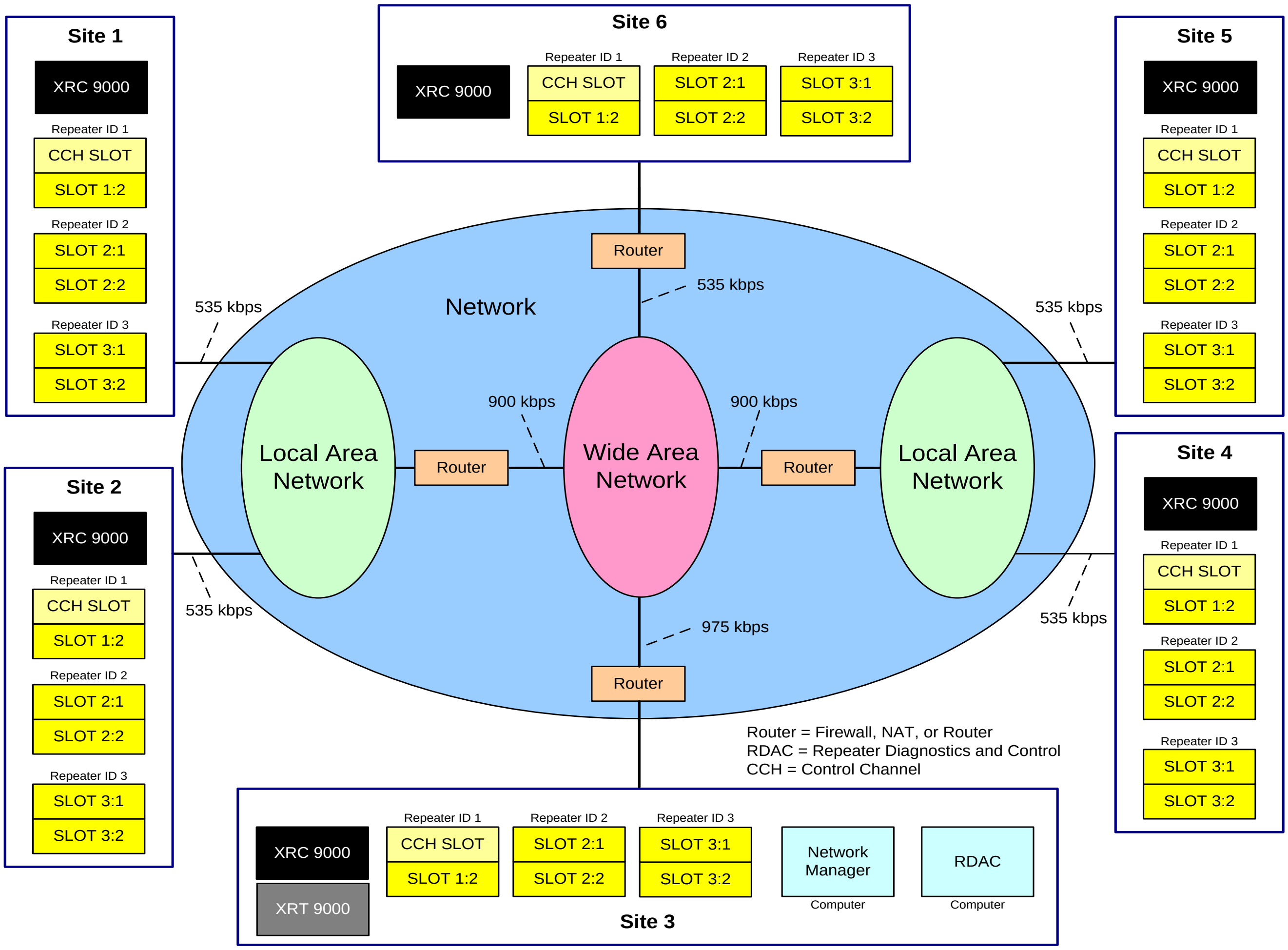
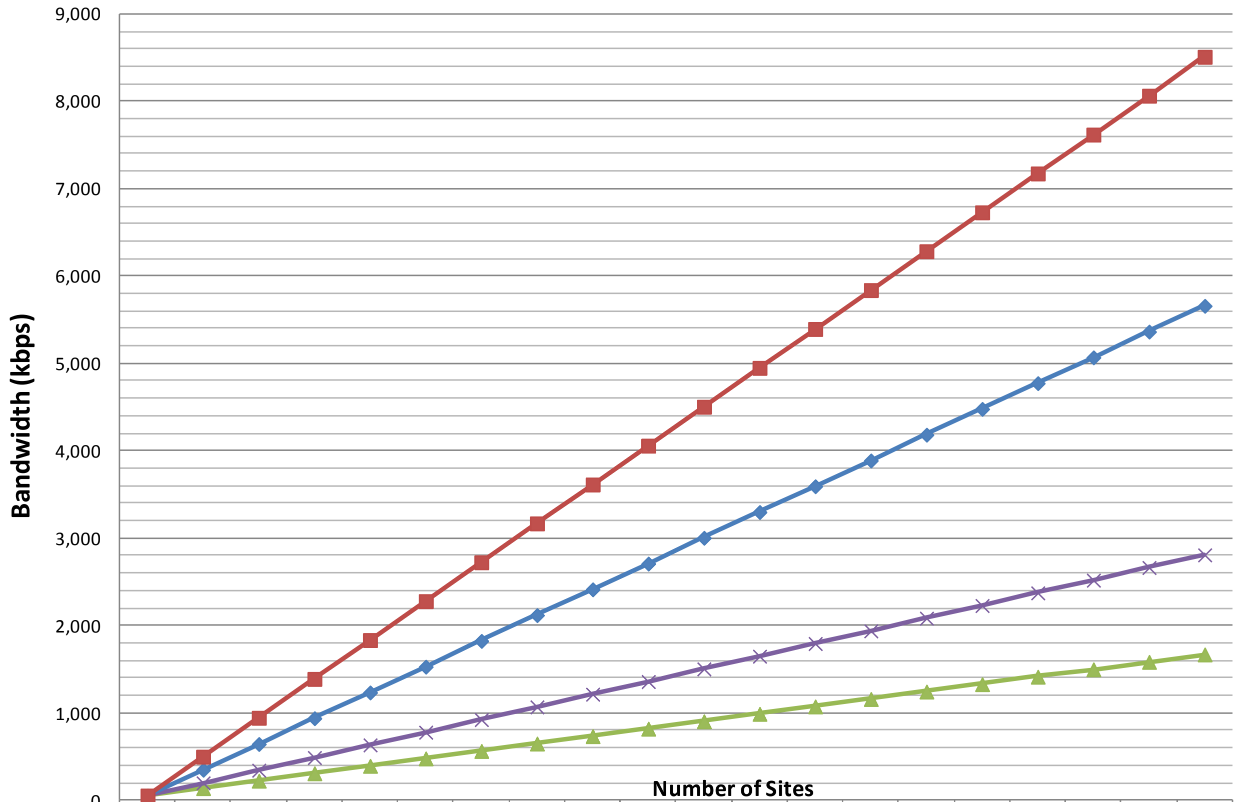


Figure 4-7 Example for Calculating Bandwidth Requirements w/o Secure VPN

The bandwidth calculations for Site 3 do not include any RDAC commands since RDAC traffic is local to the site. Another assumption is that the Network Manager at Site 3 is monitoring all 5 remote sites simultaneously and receiving streaming airtime data from each remote site; hence the additional required aggregate bandwidth is increased by 440 kbps (5 x 55 kbps + 5 x 55 kbps – 2 x 55 kbps) as compared to the other sites. Note that the aggregate bandwidth number at the router's WAN link for sites 1 and 2 is smaller than the sum of the required LAN bandwidth for site 1 and site 2; this is because these two sites do not utilize the WAN interface when communicating and routing calls between each other. The same calculations apply for sites 4 and 5.

The chart in Figure 4-8 below shows the bandwidth requirements for Connect Plus multisite system with 3, 5, 10, and 15 repeaters **per site**. Appendix D contains similar charts for more than 20 sites.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3 repeaters	55	140	225	310	395	480	565	650	735	820	905	990	1075	1160	1245	1330	1415	1500	1585	1670
5 repeaters	55	200	345	490	635	780	925	1070	1215	1360	1505	1650	1795	1940	2085	2230	2375	2520	2665	2810
10 repeaters	55	350	645	940	1235	1530	1825	2120	2415	2710	3005	3300	3595	3890	4185	4480	4775	5070	5365	5660
15 repeaters	55	500	945	1390	1835	2280	2725	3170	3615	4060	4505	4950	5395	5840	6285	6730	7175	7620	8065	8510

Figure 4-8 WAN Bandwidth Requirements for Multisite System (no VPN, no XRT)

When XRT gateway is installed on a Connect Plus network it is configured as a site with one of the reserved site IDs (251 – 255). The XRT site does not have any MOTOTRBO repeaters. It supports up to 30 simultaneous voice streams (talkpaths) to/from the XRT voice client (e.g. console). The following table provides the formula that should be used to calculate the required bandwidth for XRT.

[Max number of active calls (up to 30) to/from XRT voice client]	**X**	BW_{VC}	kbps =		kbps
[Number of Multisite sites where XRT call 1 is repeated]	**X**	BW_{VC}	kbps =		kbps
…	**X**	BW_{VC}	kbps =		kbps
[Number of Multisite sites where XRT call 30 is repeated]	**X**	BW_{VC}	kbps =		kbps
[Number of RF sites transmitting Airtime Data to XRT]	**X**	BW_{XRT}	kbps =		kbps
[Multisite control messaging for total number of sites] - 1	**X**	BW_{MC}	kbps =		kbps
Network Manager Traffic		BW_{NM}	kbps =		kbps
			+		
Required Uplink/Downlink Bandwidth					kbps

Table 4-4 Bandwidth Calculation Matrix for XRT

When XRI Interconnect Gateway is installed on a Connect Plus network it is not configured as a site in the Multisite table. The XRI site does not have any MOTOTRBO repeaters. It supports up to 16 simultaneous Telephone Interconnect calls and the bandwidth calculations are similar to those for an RF site (with XRC controller). The following table provides the formula that should be used to calculate the required bandwidth for XRI.

[Number of Multisite sites where Telephone Interconnect call 1 audio is repeated]	X	BW_{VC}	kbps =		kbps
[Number of Multisite sites where Telephone Interconnect call 2 audio is repeated]	X	BW_{VC}	kbps =		kbps
…	X	BW_{VC}	kbps =		kbps
[Number of Multisite sites where Telephone Interconnect call 16 audio is repeated]	X	BW_{VC}	kbps =		kbps
[Multisite control messaging for total number of sites]	X	BW_{MC}	kbps =		kbps
Network Manager Traffic		BW_{NM}	kbps =		kbps
[Number of active Telephone Interconnect calls][45]	X	64	kbps =		kbps
			+		
Required Uplink/Downlink Bandwidth					kbps

Table 4-5 Bandwidth Calculation Matrix for XRI

4.5.4 Required Bandwidth Calculations with VPN Configuration

As mentioned in previous sections, the initial release of Connect Plus provides only limited IP Security. Therefore, if a customer wants to secure the user communication traffic, Connect Plus supports the ability to work through a secure Virtual Private Network (VPN). Secure VPN is not a function of the Connect Plus system, but rather of the router. It is important to note that Secure VPN does add the need for additional bandwidth and may introduce additional delay. This should be taken into account when planning for bandwidth.

The following parameters should be used in the previous equation to calculate the bandwidth requirements of each device in the system when secure VPN in the routers is enabled and repeater authentication is disabled.

BW_{VC} = 23 kbps = Bandwidth required to support Multisite Voice or Data (1 slot)
BW_{MC} = 15 kbps = Bandwidth required to support Multisite control messaging
BW_{RD} = 64 kbps = Bandwidth required to support RDAC commands
BW_{NM} = 64 kbps = Bandwidth required to support Network Manager real-time monitoring
BW_{XRT} = 64 kbps = Bandwidth required to support XRT airtime data streaming mode

NOTE: The preceding data was compiled using the Linksys EtherFast Cable/DSL VPN Router with four-port switch. Model: **BEFVP41**. Other routers using different algorithms may yield different results.

4.5.5 Monitoring the Number of Network Traffic Slots

Network bandwidth requirements are not only impacted by the number of sites, but also by the number of active calls that need to be networked to other sites. This is discussed in the bandwidth calculation sections.

[45] Each digital audio (PCM) stream to/from the SIP Gateway Device requires 64 kbps of bandwidth. The SIP control traffic is ignored in the calculations.

The number of active calls on a specific site is directly influenced by the number of traffic slots available at the site. Additionally, the number of active calls, network-wide, is impacted by the number of traffic slot resources at all sites. In Connect Plus operation, a “traffic slot” is any repeater slot that is not currently being used as the Control Channel slot. Traffic slots are used for voice calls and for IP data calls such as text messages, location updates, OTA file transfer, etc.

The XRC Controller(s) and the MOTOTRBO Connect Plus Network Manager provide a feature to quickly show how many traffic slots are currently checked-in at each network site, as well as the cumulative total of all traffic slots at all connected sites. This information is provided on the Network Manger Site Status Screen. Underneath the “Traffic Slots” column, two numbers are provided, separated by a forward slash (/). The number to the left of the slash is the cumulative total of traffic slots at all sites that are currently connected to the site being viewed. The number to the right of the slash is the maximum recommended number of traffic slots, network-wide. If the actual number of traffic slots exceeds the recommended number, an exclamation mark is displayed next to “Total Traffic Slots”. If the Network Manager user places the cursor over the exclamation mark, a warning message is displayed. Exceeding the recommended number of traffic slots network-wide can have a detrimental impact on network performance and should be avoided.

4.5.6 Connect Plus IP Network Security Considerations

Network security is an important consideration. In the event that Connect Plus sites will be connected through anything other than a Private Network or Virtual Private Network, a Certified Networking Professional will need to assist the system owner in protecting the radio network from the undesired solicitations common over the public internet.

It is strongly recommended to employ the secure VPN configuration to provide high level of protection, which includes authentication and encryption. There are a slew of commercially available secure VPN routers that can be utilized to meet the network security needs of most customers. Secure VPN routers can optionally provide confidentiality of all the messages including system messages, control messages (i.e. CSBK), and voice or data headers. A disadvantage of using Secure VPN Routers is that the Connect Plus sites require more inbound and outbound bandwidth from the ISP.

4.6 Fault Management and Redundancy

4.6.1 Connect Plus Behaviors in Presence of Failures

How the Connect Plus System operates in the presence of failures depends on what type of failure is experienced. Several categories of failure will be briefly discussed:

Failure of IP connectivity between Connect Plus Sites: Connect Plus utilizes TCP/IP to send call set-up messages and other control messages between network sites. Connect Plus utilizes UDP/IP for audio routing. The XRC sends periodic messages (pings) to assess the status of TCP/IP links with other sites. These messages allow a site to know when TCP/IP communications have been lost with another site, and when TCP/IP communications have been restored. The Network Manager Site Status screen can be used to assess the status of the TCP/IP link with other network sites. For each site listed in the Multisite Details Panel, “True” indicates that there is currently a TCP/IP connection between the site to which Network Manager is currently connected and the listed site. “False” indicates that there is not currently a TCP/IP connection between the site to which Network Manager is currently connected and the listed site. It should be noted that this indicates the status of the TCP/IP connection only. When TCP/IP connectivity is normal, the XRC Controllers exchange messages with one another

that are designed to “synchronize” SU and Group records, so that each site will have an identical copy of the user database. Because of this, each site can continue to validate registrations and calls, even when cut off from part (or all) of the network due to failure of network links. During this time, audio will be heard locally, and packets can still be forwarded to linked sites. Of course, sites that do not have a current link cannot transmit the same audio, and it is possible that the same Group ID will have different conversations at different sites if there is no link to join the sites together. This will be resolved when connectivity is restored.

Failure of the XRC Controller: If an XRC failure should cause the Control Channel repeater to stop sending Control Channel messages, the site becomes “invisible” to the radios until one of the following occurs: (1) The backup XRC takes over (if the site has one), (2) The site repeaters start sending the Auto Fallback Beacon (when Auto Fallback is configured and there is no Backup XRC available), or (3) until the primary XRC is restored to service. The latter case applies when there is no Backup XRC available and when Auto Fallback is also not available (because it is not configured or is not supported by legacy software). SU’s that were registered to the site will enter Search mode. In a multisite network with overlapping site coverage, it is possible that these radios will detect and register with another Connect Plus site. If the failed site is equipped with a backup XRC, SU’s that were not able to locate a different network site will return to the original site once the backup XRC has taken over and activated the Control Channel repeater. In many cases the SU will continue using the original site without a new registration. The exception is when the SU’s Reacquire Timer expires, or if the SU attempts to register with a different network site in the interim. In those cases the SU will send a new registration to the site. If the SU is searching and detects the Auto Fallback Beacon from its configured Fallback Channel on the failed site, the radio operates in Fallback mode as described in section 4.6.5.

Failure of the Control Channel Repeater: If a Control Channel repeater failure should cause the Control Channel timeslot to stop sending control messages, the site becomes “invisible” to the radios until the XRC becomes aware of the failure and switches the Control Channel messages to a different Control Channel repeater. See the section on “Control Channel Roll-over” for more information. The SU will temporarily lose signal from the “old” Control Channel repeater before it will search for a new one. When this occurs, the Connect Plus radio looks at all the possible Control Channel frequencies for the last-registered site before it searches any other sites. If it locates an alternate Control Channel for the same site, and if the SU’s Reacquire Timer has not expired, the radio will continue using the site without a new registration. If the XRC is not aware of the Control Channel repeater failure, or if the XRC cannot start up messaging on the new Control Channel repeater before the SU begins searching other sites, it is possible that the SU will register with a different site (especially if the SU is in a location with strong overlapping site coverage). If the XRC is not aware of the repeater failure, or if there is no alternative Control Channel repeater available, the SU will continue searching until it locates a different site, or until it detects a Fallback Beacon from its configured Fallback Channel, or until service is restored. For more information on Auto Fallback, see section 4.6.5.

Failure of a trunk-to channel repeater: If a Trunk Channel Repeater fails, the observable effect to Connect Plus operation depends on whether the XRC is aware of the failure. The XRC can become aware of the failure if the repeater reports a significant alarm, or if the failure causes the repeater to stop sending “keep-alive” messages to the XRC. If the controller does not receive any repeater message prior to expiration of a timeout timer, the controller will consider the repeater to be absent, and it will no longer assign calls to the failed repeater. If the XRC is not aware of the failure, the controller will continue to assign calls to the repeater, but the calls will likely fail.

4.6.2 Connect Plus Failure Preparedness

The most important Connect Plus Failure Preparedness strategy is to provide for redundant operations by key system components.

To provide for XRC redundancy: Purchase and configure a secondary XRC controller for each Connect Plus site wherever possible. For more information, see section “XRC Redundant Controller”.

To provide for Control Channel redundancy: Configure multiple Control Channel repeaters per site (up to 4). Only one a time will be active. This strategy requires the system owner to have more than one suitable Control Channel frequency pair, and all alternative Control Channels must be configured into both the Connect Plus SU (Connect Plus CPS Network Frequency File) and the XRC (using the Connect Plus Network Manager). For more information, see section on “Control Channel Roll-Over”.

The advantage of providing a redundant XRC and redundant Control Channels is that the SU can continue to operate in trunking mode and the radio user can continue to utilize his/her normal Connect Plus features.

Another important failure preparedness strategy is the Auto Fallback feature. Auto Fallback should be used to supplement the failure preparedness strategies mentioned above (redundant XRC and redundant Control Channels), but not to replace them. Because Auto Fallback supports a very limited feature set, it should be utilized as the failure preparedness strategy of last resort. For more information on Auto Fallback, see section 4.6.5.

To provide for XRT redundancy: Purchase and configure a secondary XRT Gateway for each primary XRT Gateway. For more information, see section “XRT Redundant Gateway”.

4.6.3 XRC Redundant Controller

Each Connect Plus site requires at least one XRC Trunking Controller. The customer can purchase a second Controller per site to serve as backup to the primary Controller. The secondary controller provides backup capability, but it does not increase the number of repeaters and calls that can be managed per site. The Primary Controller can be either a XRC 9000 or a XRC 9100. The Secondary Controller can also be either a XRC 9000 or a XRC 9100.

There are some pre-requisites for utilizing the Redundant Controller feature:

1. The customer must purchase a second XRC controller. If the Multisite feature is purchased for the Primary XRC, it must be purchased for Secondary XRC also.

2. The Redundant Controller set-up requires a total of three Ethernet cables to plug into Ethernet ports on the XRCs. Standard Ethernet cables are used to connect the port labeled LAN1 on each controller to the site’s Ethernet Switch. The third cable is used to directly connect the two ports labeled LAN2 on each controller. An Ethernet crossover cable is required for the direct connection.

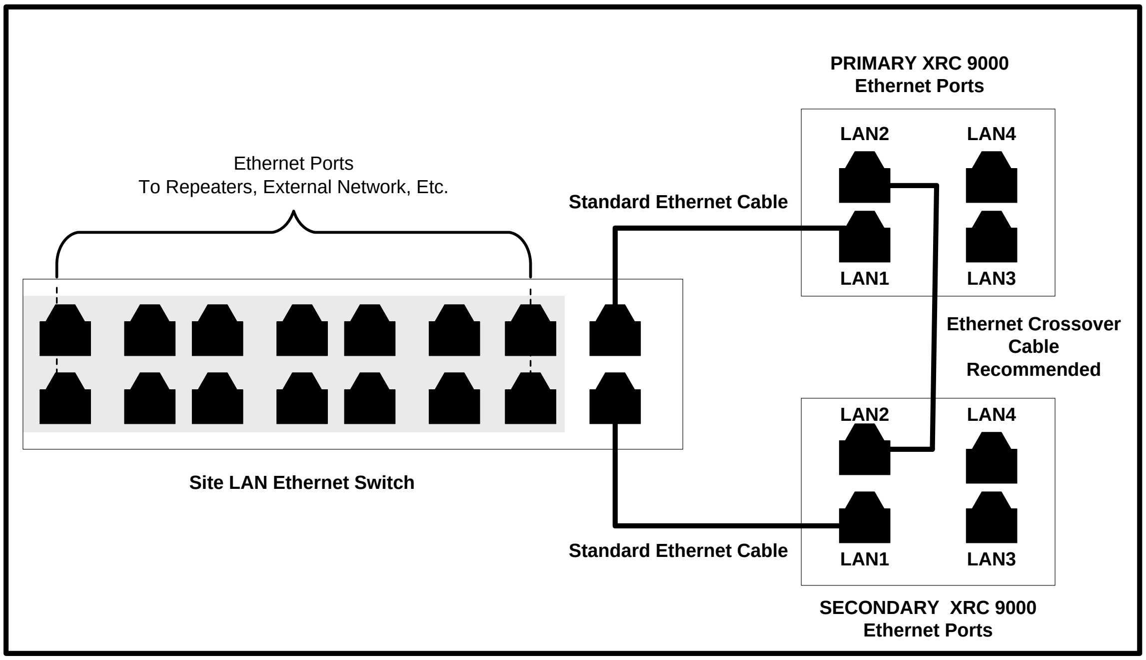


Figure 4-9 Redundant XRC: Ethernet Cable Connections

3. Except for their different roles (one configured as "Primary" and the other as "Secondary"), the two controllers require the same configuration and user information to start with. The Network Settings must be configured separately for each controller (*Network→Settings*). Other settings will be automatically shared when the Primary and Secondary XRCs are connected together and automatically synchronize certain information.

4. The Network Settings screen requires a total of 4 static IP addresses (two for each controller), as depicted in Figure 4-10 and discussed in Table 4-6.

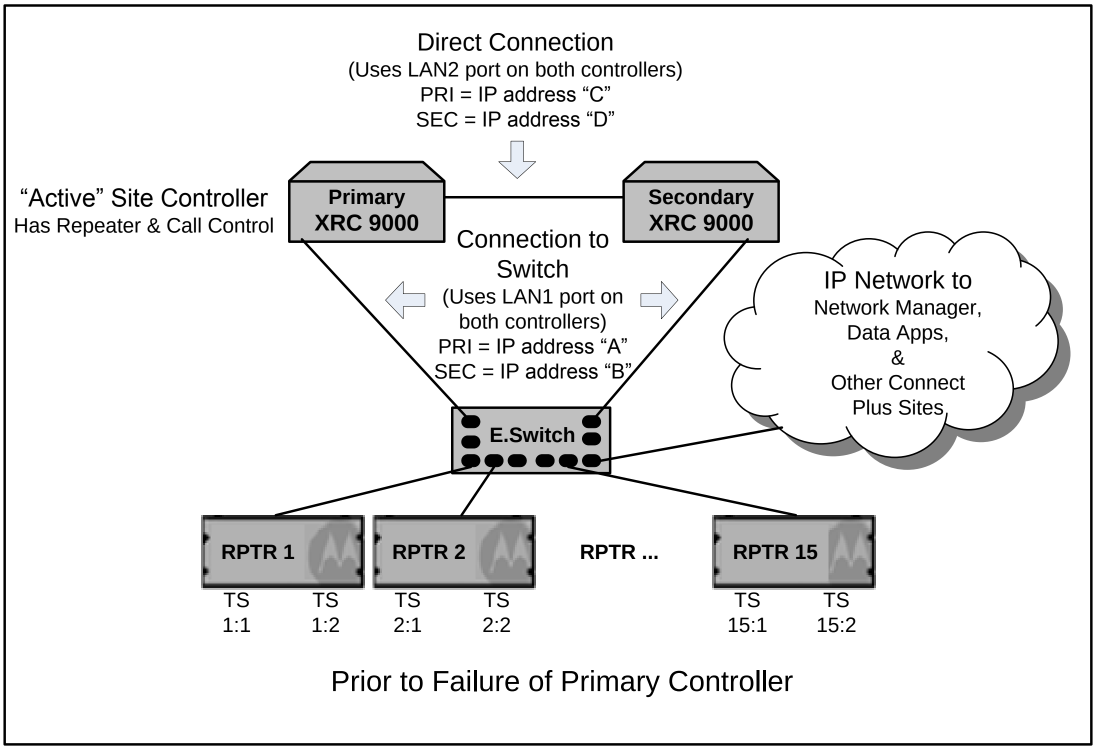


Figure 4-10 Redundant Controller Configuration with Primary XRC Active

IP Address "A" (Static IP address)	• Configured as "Primary Controller" (LAN1) IP Address • Used to address the controller that is currently "active" (has site control), regardless of whether it is the Primary or Secondary • IP address configured into the site repeaters (as IP Site Connect Master) • Multisite Tables of other Connect Plus sites point to this address • Configured "Network Properties" apply to this address
IP Address "B" (Static IP address)	• Configured as "Secondary Controller" (LAN1) IP Address • Used to address the controller that is currently "inactive" (does not have site control), regardless of whether it is the Secondary or Primary • Configured "Network Properties" apply to this address
IP Address "C" (Static IP address)	• Configured as "Primary Controller" (LAN2) IP Address • Used only for the direct connection between the two XRC controllers. Only the two controllers know about this address. • Always belongs to the Primary Controller, regardless of whether it is "active" or "inactive" • First three octets of this address must be exactly the same as first three octets of IP address "D" (Secondary Controller [LAN2] IP address). • First three octets of this address must be different than the first three octets of IP Address "A" and IP Address "B". • Configured "Network Properties" do not apply to this address
IP Address "D" (Static IP address)	• Configured as "Secondary Controller" (LAN2) IP Address • Used only for the direct connection between the two XRC controllers. Only the two controllers know about this address.

	• Always belongs to the Secondary Controller, regardless of whether it is "active" or "inactive" • First three octets of this address must be exactly the same as first three octets of IP address "C" (Primary Controller [LAN2] IP address). • First three octets of this address must be different than the first three octets of IP Address "A" and IP Address "B". • Configured "Network Properties" do not apply to this address
Notes:	• The Primary & Secondary controllers can automatically "swap" Addresses A & B in switchover scenarios, but the Network Manager configuration remains the same. • The Primary & Secondary never "swap" Addresses C & D

Table 4-6 XRC IP Addresses

Basic Concepts

Controller Roles that can be configured in the Network Manager

Every XRC has one of three "roles" as discussed below:

- **Stand-alone**: This is the role of a controller that doesn't have any redundant backup. It is the default controller role, and will not change unless the Network Manager is used to configure a different role.

- **Primary**: This is the role assigned to the controller that should be in charge while the site is operating normally. Once assigned the Primary role via the Network Manager, it is always referred to as the Primary controller – even if the Secondary controller detects a fault and takes over.

- **Secondary**: This is the role assigned to the controller that should be in "stand by" while the site is operating normally. Once assigned the Secondary role via the Network Manager, it is always referred to as the Secondary controller – even if it takes over site control.

Non-configurable states

In conjunction with the configurable roles, there are two important non-configurable Site Control states:

- **Active Controller**: This is the controller currently in charge of site control (repeaters, calls, etc), regardless of whether it is the Primary or Secondary

- **Inactive Controller**: This is the controller currently not in charge of site control (repeaters, calls, etc), regardless of whether it is the Secondary or Primary.

    - While the Secondary Controller is inactive, it is usually (if configured & connected correctly) in "standby" mode – ready to take over site control if there is a failure of the Primary controller.

    - While the Primary Controller is inactive, it is not in "standby" mode. It will not automatically switch back to being the active controller. For switch back to occur, the "Switch to Primary Controller" command must be sent using the Network Manager software.

Creating Connections for MOTOTRBO Connect Plus Network Manager Connection Tool

1. Use the MOTOTRBO Connection Tool to create a connection pointing to the Primary Controller LAN1 IP address (IP Address "A" in the preceding table).

   a. The Network Manager uses this connection for communicating with the active Site Controller (i.e. currently in charge of repeaters and calls assignment). This could be either the Primary or Secondary controller. The site box on the Site Dashboard will show whether the Network Manager connects to the Primary or Secondary controller via this IP address.

   b. This connection can be placed in the Connection Group that contains all network sites. Using this connection, the Network Manager will automatically connect to the site's active controller.

2. Use the MOTOTRBO Connection Tool to create a connection pointing to the Secondary Controller LAN1 IP address. (IP Address "B" in the preceding table).

   a. This connection is used for communicating with the inactive Site Controller (i.e. not currently in charge of repeaters and calls assignment). This could be either the Secondary or Primary controller. The site box on the Site Dashboard will show whether the Network Manager connects to the Secondary or Primary controller via this IP address.

   b. To avoid confusion, do not place this connection in the Connection Group that contains all network sites. Use the Connection Tool's single connection feature when it is necessary to communicate with the inactive site controller. An alternative approach is to create a separate Connection Group for each site that includes both the Primary and Secondary Controller LAN1 IP connections for the site.

3. Do not create connections pointing to the LAN2 IP addresses (IP Address "C" and "D" in the preceding table). These ports are used for direct controller-to-controller communication.

Determining the Role and State of the connected XRC

When connecting to a XRC with the Network Manager, it is very important to know the controller's role (Primary/Secondary) and current site control state (Active/Inactive). The Site Dashboard shows the controller's role and site control state at the bottom of the box representing the connection. Each connected XRC will have one of the following labels:

- Stand-alone (A Stand-alone is assumed to be in site control. So, no additional state is provided)

- Primary / Active
- Secondary / Inactive

- Secondary / Active
- Primary / Inactive

Important! If any changes need to be made to the XRC configuration, such changes should be configured into the active XRC. The active XRC will automatically share the changes with the inactive XRC controller. Do not individually configure any User Settings or Site Configuration parameters while connected to the inactive XRC. There is too much chance that such changes will never take effect, or will be overwritten by values in the active XRC, or overwritten by user configuration changes from other sites.

Maintaining the Primary and Secondary Controllers at same Firmware level

It is important to maintain the Primary and Secondary controllers at the same XRC firmware version.

- Make sure the Primary and Secondary controllers are at same firmware level prior to initial deployment of Redundant Controllers at the site.

For field upgrades, both controllers should be upgraded when upgrading to a new XRC firmware build. (Note: This requires two separate files because each XRC must always have its own firmware file. The file name should be the same except for the serial number, which is the last part of the file name.)

Configuring the Primary and Secondary Controller

It is recommended to perform initial configuration at the shop, prior to installing the XRC(s) at the site. In the case of an existing site, only the Secondary controller needs to be configured at the shop, since the Primary went through this process prior to its original deployment. Some configuration is still required for the Primary controller, but this can be accomplished at the site if necessary.

As a general rule of thumb, do not connect the XRCs directly (Lan2 on Primary to Lan2 on Secondary) until both controllers have been fully configured and are ready for redundant operation. This will help prevent the Secondary controller from attempting to assume site before you are ready. The Secondary controller will not attempt to take over site control until it has synched at least one time with the Primary via the LAN2 connection.

The following outline shows the steps that must be performed before the Redundant Controller feature will be operative. Do not connect the LAN2 ports prior to the point mentioned in the outline. This outline assumes that at least one controller has been previously configured for site control. If this is not the case, follow the installation and configuration guidelines outlined in the XRC User Guide.

1. Configuring the Secondary Controller

    a. If the Secondary Controller is “fresh out of the box”, the first step is to establish communication with the controller. Because the controller comes with a default IP address, you may have to edit the IP address on your PC for the first connection. See the XRC User Guide for details. When initially configuring the IP address that will be used for this controller, enter the address into the Primary IP Address field (for LAN 1) and leave the controller role as “stand-alone”. In a later step, the controller role will be changed to “Secondary”, and its IP address will be configured into the Secondary IP address field (for LAN 1).

    b. The Network Time Protocol (NTP) Configuration for the two controllers that will serve as Primary and Secondary for the same site must be configured the same. If the Primary will serve as the network’s NTP Server, then the Secondary must also be configured as network’s NTP Server. If the Primary is configured point to another IP address as NTP Server, then the Secondary must also point to the same NTP Server.

    c. Manually set the clock on the XRC that will serve as the Secondary Controller in order to bring it as close as possible to the NTP Server time. This important step helps this XRC to synch its time with the NTP server more quickly (once a connection is established to the NTP Server). Set the date and time from the Date Time Configuration screen (*Settings→Date and Time*).

    d. Configure the settings on the Controller TCP/IP screen of the Secondary Controller for field operation (*Network→Settings*).

        i. Set the Controller Role as “Secondary”.

        ii. Configure Network IP Addresses, Network Properties, and Redundant Controller Feature IP Addresses to be used at the site. It is important to note that these fields must be configured with identical information in both the Primary and Secondary controller, and that the configured values do not change – even when the Secondary controller automatically assumes the Primary controller’s IP address and becomes the “active” site controller.

e. After saving the Network Settings the Secondary Controller will reboot and come back with its new IP address. It will probably be necessary to make one or more changes (such as editing the PC's IP address, re-defining the connection information in the Connection Tool, taking the controller to the site, etc) prior to communicating with this XRC again.

2. Configuring the Primary Controller. (Instructions assume that this is an operating site controller that has already been configured with most settings.)

   a. Connect to the XRC that will be used as Primary Controller.

   b. Since it is important to always have a current backup file for each Connect Plus site, use the Network Manager Backup & Restore Utility to make a backup file of this controller (*Settings→Backup & Restore Utility*). Do not be concerned about performing the backup prior to configuring the Controller TCP/IP screen as described in the next step. That information is intentionally omitted from the backup file.

   c. Open the Controller TCP/IP screen (*Network→Settings*).

      i. Configure the Controller Role as "Primary"

      ii. Configure Network IP Addresses, Network Properties, and Redundant Controller Feature IP Addresses to be used at the site. It is important to note that these fields must be configured with identical information in both the Primary and Secondary controller, and that the configured values do not change – even when the Secondary controller automatically assumes the Primary controller's IP address and becomes the "active" site controller.

   d. After saving the Network Settings the Primary Controller will reboot. It will be necessary to re-connect, if desired.

Making the physical connections (assumes that configuration is complete)

Follow the steps below after completing the configuration described in the previous section:

1. Bring both controllers to the site location (if not done already)

2. For an existing site, the Primary controller will already be connected to the Ethernet switch.

3. Connect the Secondary Controller to the Ethernet switch (from LAN1 port on controller).

4. Plug in the direct connection between the two ports labeled "LAN2" on the Primary and Secondary controllers.

5. Provide power to the Secondary Controller. After the Secondary Controller finishes booting up, it will communicate with the Primary Controller. The Primary and Secondary controller will then start the process of synchronizing important settings. This process can take several minutes, depending on how much information needs to be shared. See the next section for more information.

Important! Prior to leaving the site, it is strongly recommended that the technician perform a test to verify the redundant operation. The specific instructions for this test are provided in a later section.

Primary and Backup Controllers synchronize certain information

After establishing the direct connection between the Primary and Secondary controller, the two XRCs will automatically synchronize the following important information:

1. If the user database is not already identical in both controllers, then the user database from the active XRC will replace the user database in the inactive XRC. This process can take up to five minutes, depending on the size of the user database in the active controller. If the user database in both controllers is already identical, this step is omitted.
2. Settings contained on the active controller's (Site) Configuration Screen will replace the Site Configuration settings for the inactive controller.
3. Settings contained on the active controller's Multisite Configuration Screen will replace the Multisite settings for the inactive controller.
4. The list of repeaters currently checked in with the active controller.
5. The Radio ID of the repeater currently acting as Control Channel repeater.
6. The list of units and groups currently registered into the network, as well as their present site location.
7. User Roles (Login accounts) are shared from the active to inactive controller.
8. SMTP Setup and Alert Notifications that have been configured into the active controller will replace the SMTP Setup and Alert Notifications settings for the inactive controller.
9. The Primary Controller's "Site Reset" count. The "Site Reset Count" is maintained behind-the-scenes to help SUs know when they are required to re-register with a site. It is not the same thing as the "Number of site reboots", which can be viewed with the Network Manager.
10. Certain network messages that have been sent to other sites, but have not yet been acknowledged by the destination site.
11. Location update schedules and undelivered text messages for subscriber units currently registered to this site.

In order to determine when the synch process is complete, connect to the Primary Controller with the Network Manager and view the Alert/Alarms Management Screen (*Alerts/Alarms→Alerts/Alarm Management*). The Primary Controller will show a Controller Alert that says, "Primary Controller missing connected Secondary Controller". Press the "Clear" button to clear this Alert, and then wait for five seconds and press the "Refresh" button. If the Alert does not reappear, then the synch process is complete, and the Secondary Controller is ready to assume site control when needed.

Continued Sharing of Information

Following their initial synchronization, the active controller continues to automatically update the inactive controller when certain changes occur:

Following their initial synchronization, and for as long as the active and inactive controllers have a LAN2 connection, the active controller continues to automatically update the inactive controller when changes to any of the information that was shared during the initial synchronization process described in the previous section.

The active XRC also informs the inactive controller whenever a user initiates a voluntary site reset of the active controller. The term “voluntary reset” includes the following:

1. Reboot command issued via Network Manager.

2. A “critical” setting is updated via Network Manager and saved to XRC. This includes the following:
   a. Any setting in “Critical Settings” portion of Configuration screen (*Settings→Configuration*).
   b. Any setting on Controller TCP/IP screen (*Network→Settings*).
   c. Any setting on Multisite Configuration screen (*Settings→Multisite*).

3. Saved configuration file is uploaded via Network Manager.

4. Firmware Upgrade command issued via Network Manager.

Following a voluntary reset, an Inactive Secondary Controller allows the Primary Controller a period of time to reboot and resume site control. If the Primary XRC does not come back on line within the expected period of time, the Secondary Controller will attempt to take over site control.

Information not shared

It is also important to understand that there is some information that is automatically not shared between the active and inactive controllers. This includes the following:

1. Information on current calls (assigned calls and calls in the Busy Queue). These do not carry over when there is a switchover in site control from the active to the inactive controller.

2. The list of active network connections with sites listed on the Multisite Table. (When a controller takes over site control, it will attempt to set-up new connections with all sites on its Multisite Table.)

3. Airtime Logging Data. This is only saved to the currently active controller.

4. Event Log Data. This is only saved to the currently active controller.

5. Unexecuted File Transfers. These must be re-uploaded following a switch in site control.

6. Controller Alerts & Repeater Alarms on the other XRC

   a. Active controller alerts will re-trigger after new controller assumes site control.

   b. Active repeater alarms will be discovered at next Link Establishment (LE) or when reported by repeater

7. Undelivered data packet(s) sent by an XRT Client awaiting delivery to a Connect Plus SU. The XRT Client can resend the packet(s), if desired, if the XRT doesn’t provide a notice of transmission within an expected period of time.

Automatic Switch of Site Control

The active and inactive controllers exchange heartbeat messages over their LAN2 direct connection. The switchover from Primary to Secondary can be triggered by the loss of heartbeat messages between the two controllers, or by the loss of heartbeat messages between all peer repeaters and the Primary XRC. Because heartbeat messages between the two XRCs are sent at a much higher frequency than heartbeat messages between the Primary XRC and the peer repeaters, XRC failure can be detected in just a few seconds, whereas it takes somewhat longer to detect a failure of the IP interface between the Primary XRC and all repeaters.

In summary, automatic switchover is supported for the following scenarios:

1. Any scenario that results in the loss of heartbeat messages between an active Primary and inactive Secondary controller. Examples include (1) power failure on Primary XRC (2) Hardware failure affecting IP ports on Primary XRC, (3) Connect Plus software program stops running on Primary XRC. Switchover occurs following expiration of an internal timer in the Secondary XRC (approximately 3 seconds).

2. Any scenario that results in the loss of heartbeat messages between an active Primary controller and all of its peer repeaters AND the Secondary controller is simultaneously unable to communicate with the Primary controller over the LAN 1 network. Switchover will occur following expiration of an internal timer in the Primary XRC (approximately 16 seconds). It is important to note that depending on where the failure occurred in the IP interface, it may also be impossible for the Secondary XRC to communicate with the peer repeaters. In this event, switchover will occur, but radio communications will still be down.

Note: There are some scenarios where the Secondary XRC may attempt to take over site control, but not be able to so. An example of such a case is when the LAN2 connection between the two controllers fails, but the Primary Controller still has a good LAN1 connection to the site repeaters. In this event, the Primary Controller will continue to control the site, and it will not relinquish its Primary Controller LAN1 IP address. If the Secondary XRC attempts to take over site control due to a Failover Trigger, but is not able to take over the Primary Controller IP address, it will create an Event Log entry and periodically retry.

Figure 4-11 illustrates Redundant Controller connections after site control switches from the Primary to Secondary controller.

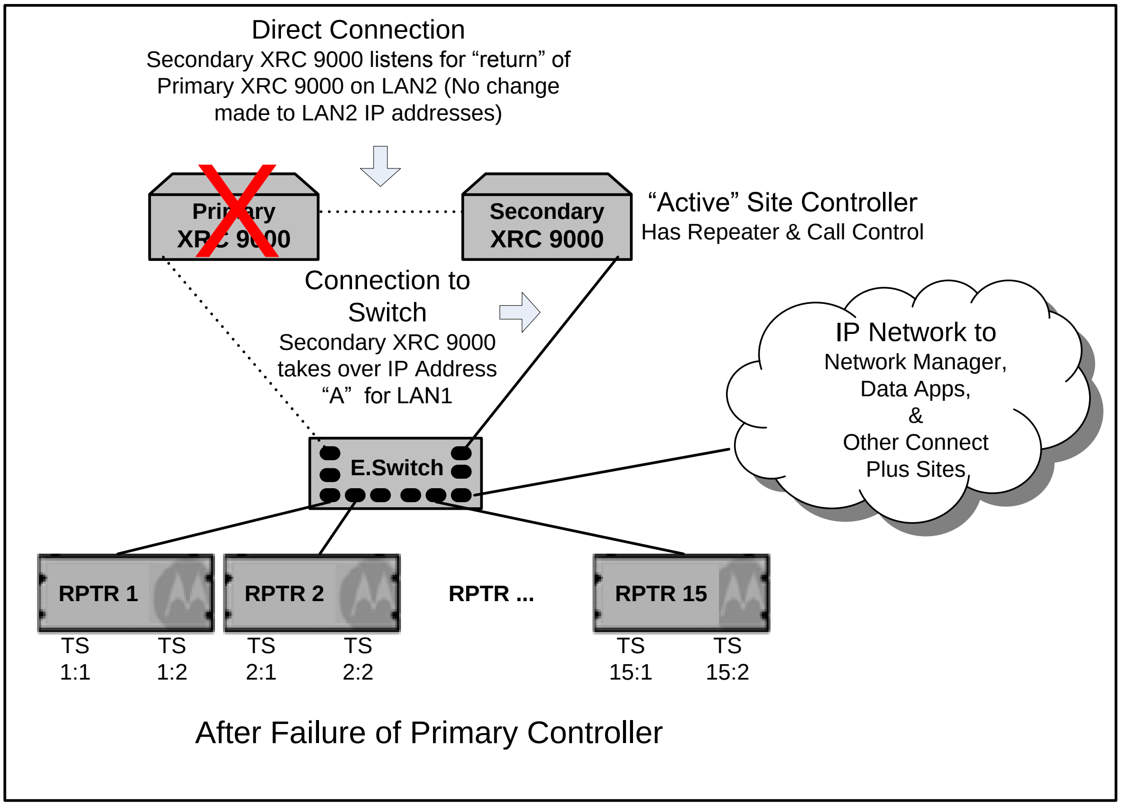


Figure 4-11 Redundant Controller Configuration with Secondary XRC Active

Swapping LAN1 IP Addresses

Whenever a controller switchover occurs, the (newly) active XRC controller will take-over the IP address that has been configured with Network Manager as the "Primary Controller IP Address" for LAN1. (IP Address "A" in the preceding table.) In other words, this is the IP address for the "active" controller, regardless of whether it is the Primary or Secondary.

If a XRC attempts to use the IP address that has been configured with Network Manager as the "Primary Controller IP Address" for LAN1, but finds out the address is already in use, it will assume the "inactive" state, and will instead use the IP address that has been configured with Network Manager as the "Secondary Controller IP Address" for LAN1. An example of such a case is when the Secondary Controller has taken over site control, and then the Primary controller subsequently comes back on line. The Primary Controller shall make one attempt to use the Primary Controller IP address. Upon finding that the "Primary" address is already in use, the controller will use (or attempt to use) the "Secondary" address for as long as it remains in the "inactive" state, even though its configured role remains that of "Primary Controller".

In order to swap IP addresses as described in this section, the site's LAN Ethernet switch must be able to accept a gratuitous ARP response, and change a previously registered IP address. If there is any question about whether the site's Ethernet switch will accept gratuitous ARP responses, check the switch configuration or consult the company IT specialist. A subsequent section describes a test that, if passed successfully, confirms that the site's LAN Ethernet switch accepts gratuitous ARP responses.

Site Control switch initiated via the Network Manager

In addition to the failure scenarios that cause automatic switchover from the Primary to Secondary controllers, switchover can also be initiated via a Network Manager Menu command. The switchover command should always be given to the active controller. It is useful for the following:

1. Technician wishes to switch site control from Primary to Secondary controller in order to perform maintenance on Primary controller.

2. Technician wishes to switchover site control from an active Secondary controller back to the Primary controller (usually after completing repair or replacement of Primary controller). Because there is no automatic switchover from Secondary to Primary, the Menu command is the only way this can be accomplished. If it is necessary to replace the former Primary Controller with another XRC, use the Network Manager to perform some basic configuration on the (new) Primary Controller prior to switching site control back to the Primary. Perform the following configuration at the shop prior to bringing the (new) Primary Controller to the site:

    a. If the (new) Primary Controller is “fresh out of the box”, the first step is to establish communication with the controller. Because the controller comes with a default IP address, you may have to edit the IP address on your PC for the first connection. See the XRC User Guide for details. When initially configuring the IP address that will be used for this controller, enter the address into the Primary IP Address field (for LAN 1) and leave the controller role as “stand-alone”. In a later step, the controller role will be changed to “Primary”, and its IP address will be configured into the Primary IP address field (for LAN 1).

    b. The Network Time Protocol (NTP) Configuration for the two controllers that will serve as Primary and Secondary for the same site must be configured the same.

    c. Manually set the clock on the (new) Primary XRC in order to bring it as close as possible to the NTP Server time. Set the date and time from the Date Time Configuration screen (*Settings→Date and Time*).

    d. Configure the Controller TCP/IP Screen of the (new) Primary Controller for field operation (*Network→Settings*).

        i. Set the Controller Role as “Primary”.

        ii. Configure Network IP Addresses, Network Properties, and Redundant Controller Feature IP Addresses to be used at the site. It is important to note that these fields must be configured with identical information in both the Primary and Secondary controller.

    e. After completing the configuration above at the shop, transport the (new) Primary XRC to the site location, connect its LAN1 port to the LAN Ethernet Switch, connect its LAN2 port directly to the LAN2 port on the active Secondary XRC (using the Ethernet Crossover Cable), and apply power to the (new) Primary XRC. The (new) Primary XRC will discover that the Primary Controller IP Address is already in use. It will go the “inactive” state, and it will use the Secondary Controller LAN1 IP address. When the two controllers establish communication via their LAN2 connection, the controllers will synchronize important settings as described previously. In this scenario, the settings in the active Secondary XRC take precedence and will replace the settings in the inactive Primary XRC.

    f. When the two controllers have finished the synch process, use the Network Manager to connect to the active Secondary XRC (using the Network Manager connection for the Primary Controller IP Address), and give the “Switch to Primary Controller” command (*Site Control→Switch to Primary Controller*).

Note: If the technician attempts to manually switch site control by using either the “Switch to Primary Controller” or “Switch to Secondary Controller” command before the two controllers have completed the synch process, the Network Manager returns a message that says, “The controller rejected the switch command”. Should this occur, wait a few minutes and then attempt to give the switch command again.

Site operation during switchover

The switchover process causes an interruption to site communications. Calls in progress and calls in the Busy Queue are not maintained through a controller switchover. Following switchover, the (new) active controller will re-establish links to other network sites. SU operation is described in the next section.

SU operation during switchover

If a Connect Plus SU is transmitting voice at time of switchover, it will continue to transmit until PTT is released. Then it will enter Search mode. If a Connect Plus SU is listening to a call at switchover, the call will drop and the SU will enter Search mode. If the SU is idle when switchover occurs (not in a call), it will enter Search mode.

When switchover causes the Connect Plus SU to enter Search mode, the SU will follow its normal Search logic.

In Networks with overlapping site coverage, Connect Plus SUs may register with other network sites before the new active controller starts up Control Channel messaging. If there is no overlapping coverage (or in a single site system), the Connect Plus SU will come back to the same site and use the new active controller. Because the (formerly) active controller shared its registration list prior to the switchover, the Connect Plus SU does not need to send a registration to the new active controller. However, whether the SU sends a registration to the controller, or whether the SU starts using the site without a registration is determined through the SU’s normal rules:

- If SU has not attempted to register with another site in the interim, and if the SU’s configured Reacquire Timer has not expired, the SU will begin using the site without a registration.

- If SU has attempted to register with another site in the interim, or if the SU’s configured Reacquire Timer has expired, the SU will send a new registration prior to using the site.

Determining XRC Status

The XRC and the Network Manager provide several indications to determine a controller’s current status and whether a switchover has occurred on the site:

Network Manager Site Dashboard: As discussed previously, when the Network Manager connects to a XRC, the Site Dashboard tells the “role” of each connected XRC. If the “role” is “Primary” or “Secondary”, the dashboard also tells the current state, “active” or “inactive”.

Event Log Entries: When the Secondary controller has established connectivity to the Primary controller, and then has subsequently lost the heartbeat messages for a period of time, the Secondary controller writes a “Controller Absent” message to the Event Log. This entry is created by the Primary Controller when it loses its connection to the Secondary Controller, or when the Secondary controller fails to connect after an expected period of time following boot-up. This entry is also created by the Primary controller if it loses connectivity to all of its peer repeaters for a period of time, and cannot instruct the Secondary controller to take over site operation.

When either the Primary or Secondary controller switches states (inactive to active, or vice versa), it places a “Controller Switch State” entry in the Event Log. The message shows the controller’s state, active or inactive.

The inactive controller will create a “Controller Switch State Failure” Event Log entry if it attempts to switch to the active state, but is not able to take over the Primary Controller LAN1 IP address.

Controller Alerts: Controller Alerts can be viewed on the Network Manager's Alerts/Alerts Management Screen of the active site controller. Controller Alerts do not clear automatically on the active controller. They must be cleared by the System Administrator or Technician after determining that the condition which triggered the Alert no longer exists. If the underlying trigger still exists, the Controller Alert will return.

Alerts/Alarms can be viewed and managed on the active controller only. They cannot be viewed or managed on the inactive controller. When a controller changes to the inactive state, it clears any Controller Alerts that may have been active on that XRC.

There are two alerts associated with Redundant Controller operation.

> *Primary Controller missing connected Secondary Controller*: This alert indicates that the Primary Controller has not yet communicated with the Secondary Controller, or that communication has been established, but the process of synching with the Secondary Controller is not yet complete. For more information about his Alert, see the section called "Primary and Backup Controllers synchronize certain information".
>
> *Secondary Controller Active*: This alert is generated when the Secondary Controller takes over site operations.

Testing the switchover capability

After configuring and connecting the redundant controllers, the technician should test switchover functionality, using the same the same LAN Ethernet switch that is used (or will be used) at the site. The steps for the test are listed below. The test will cause an interruption to radio service at two points (switchover from Primary to Secondary, and switchback from Secondary to Primary). For this reason, it should be performed at a time when site activity is low.

1. Complete all configuration and connections as described previously.
2. Use Network Manager Connection Tool to connect to the IP address that has been configured into the controllers as the Primary Controller IP address for LAN1.
3. After making the connection, look at the box representing the connected controller in the Site Dashboard. At the bottom of this box it should say, "Primary/Active".
4. Click on the box representing this controller in the Site Dashboard. The box turns blue and "selects" the XRC for configuration.
5. From the Main Menu, select *Site Control→Switch to Secondary Controller*
6. Acknowledge the warning message. This will reset the XRC and disconnect you from the site.
7. The switchover takes place, causing a temporary interruption to service. Calls-in-progress will drop and the subscriber units will enter Search mode. If the site has overlapping coverage with another network site, some SUs may change sites during the switchover.
8. Use Network Manager Connection Tool to connect to the IP address that has been configured into the controllers as the Primary Controller IP address for LAN1.
9. After making the connection, look at the box representing the controller in the Site Dashboard. At the bottom of this box it should say, "Secondary/Active". Assuming that you are connected via the site's LAN Ethernet Switch, this confirms that the switch accepted the secondary's gratuitous ARP response.

10. Click on the box representing this controller in the Site Dashboard. The box turns blue and “selects” the XRC for configuration.
11. From the main menu, select *Alerts/Alarms→Alert Management*. This opens the Alerts/Alarms Management screen. There should be an active Controller Alert for “Secondary Controller Active”.
12. From the Main Menu, select *Site Control→Switch to Primary Controller*
13. Acknowledge the warning message. This will reset the XRC and disconnect you from the site.
14. The switchover takes place, causing a temporary interruption to service. Calls-in-progress will drop and the subscriber units will enter Search mode. If the site has overlapping coverage with another network site, some SUs may change sites during the switchover.
15. Use Network Manager Connection Tool to connect to the IP address that has been configured into the controllers as the Primary Controller IP address for LAN1.
16. After making the connection, look at the box representing the controller in the Site Dashboard. At the bottom of this box it should say, “Primary/Active”. Assuming that you are connected via the site’s LAN Ethernet Switch, this confirms that the switch accepted the primary’s gratuitous ARP response. Site Control has now been returned to the Primary.

4.6.4 Monitoring Faults in the Connect Plus System

Each XRC maintains an “Event Log”, which can be downloaded and viewed using the MOTOTRBO Connect Plus Network Manager. Not all Event Log entries are system errors. When the Event Log archive exceeds a size of 20 MB, the oldest entries are automatically purged.

Some (but not all) error conditions cause the XRC to raise a “Controller Alert” or “Repeater Alarm”. This is a more aggressive form of fault notification, and the user will be alerted via the Network Manager’s Site Dashboard upon establishing connection with the site.

Each XRT maintains an “Event Log”, which can be downloaded and viewed using the XRT Configuration Tool software. Not all Event Log entries are system errors. When the Event Log archive exceeds a size of 20 MB, the oldest entries are automatically purged.

Some (but not all) error conditions cause the XRT to raise an Alert. This is a more aggressive form of fault notification, and the user will be alerted via the XRT Configuration Tool’s Alerts/Alarms Management Screen.

Controller Alert: A Controller Alert is raised when certain underlying fault conditions occur. There may be several different faults that than can trigger the same category of Controller Alert. For example, any Repeater Alarm reported by the repeater to the XRC will raise the “Repeater Alarm Detected” Controller Alert. It is necessary to view the site’s Event Log to see which specific repeater alarm may have raised the Controller Alert. Because a Controller Alert “latches” until the technician clears the alert via the Network Manager, the underlying fault may or may not still be active.

Repeater Alarm: Repeater Alarms indicate some type of fault in repeater operation. In most cases, the repeater reports the alarm to the XRC, which causes the controller to create an Event Log entry for the specific alarm and to raise the generic “Repeater Alarm Detected” Controller Alert (if not already active). Depending on severity, Repeater Alarms may or may not result in an interruption to service. In all cases, the underlying fault should be further investigated. Repeater Alarms differ from Controller Alerts in a couple of important ways:

1. If a Repeater Alarm is displayed, the underlying fault is likely still active. (It is possible that the fault has been addressed, but the repeater has not yet reported this to the XRC.)

2. The technician cannot clear the Repeater Alarm from the Network Manager application. The Repeater Alarm must be cleared in some other fashion. The XRC will clear the alarm if the repeater reports that the alarm is no longer active, or if the repeater completes a subsequent Link Establishment and the alarm is no longer active.

The XRC can be configured to automatically send an email when a "Controller Alert" is triggered in the XRC. This functionality requires some configuration in the XRC, and the customer must have a SMTP server that the XRC can reach via IP.

Regardless of whether the customer becomes aware of a Controller Alert via the Network Manager Site Dashboard, or via an email, it is important to understand the following important points about Controller Alerts:

- The Alert notification contains very few details. Its purpose is to alert a significant person (such as a technician) that there is a problem that needs further investigation. The technician must use the Network Manager connect to the site so that he/she can investigate further. For many Controller Alerts, there will be an Event Log entry for the event that triggered the alert.

- Once an event occurs to trigger a Controller Alert, the Controller Alert latches "on" until manually cleared via the Network Manager (even if the underlying fault has been corrected).

- If the Controller Alert is manually cleared, but the underlying fault has not been corrected, the Controller Alert will likely be triggered again.

- As long as the Controller Alert remains latched in the "on" position, subsequent faults in the same category do not re-trigger the alert. One ramification of this operation is as follows; the XRC will not send emails for subsequent faults in the same Controller Alert category until the previous Alert has been manually cleared via the Network Manager.

- If a site has two controllers in redundant controller configuration, Alerts/Alarms can be viewed and managed on the active controller only. They cannot be viewed or managed on the inactive controller. When a controller changes to the inactive state, it clears any Controller Alerts that may have been active on that XRC.

- The XRC Controller supports a "System Health Alert". This alert is raised upon detection of certain conditions that may be detrimental to hardware or software performance. When the alert is raised, an Event Log entry is also created. The Event Log entry contains a "System Health issue number" that can be provided to Motorola Solutions technical support personnel for further investigation.

Gateway Alert (XRT): The XRT Gateway supports Gateway Alerts. A Gateway Alert is raised when certain underlying fault conditions occur. It is recommended to view the Event Log for more information about the event that prompted the Alert. Because an Alert "latches" until the technician clears the alert via the XRT Configuration Tool, the underlying fault may or may not still be active.

The XRT can be configured to automatically send an email when an Alert is raised. This functionality requires some configuration in the XRT, and the customer must have a SMTP server that the XRT can reach via IP.

It is important to understand the following important points about Alerts:

- The Alert notification contains very few details. Its purpose is to alert a significant person (such as a technician) that there is a problem that needs further investigation. The technician must use the XRT Configuration Tool to connect to the XRT so that he/she can investigate further. For most Alerts, there will be an Event Log entry for the event that triggered the alert.

- Once an event occurs to trigger an Alert, the Alert latches “on” until manually cleared via the XRT Configuration Tool (even if the underlying fault has been corrected).

- If the Alert is manually cleared, but the underlying fault has not been corrected, the Alert will likely be triggered again.

- As long as the Alert remains latched in the “on” position, subsequent faults in the same category do not re-trigger the alert. One ramification of this operation is as follows; the XRT will not send emails for subsequent faults in the same Alert category until the previous Alert has been manually cleared via the XRT Configuration Tool.

- If there are two XRT Gateways in Redundant Gateway configuration, Alerts can be viewed and managed on the active Gateway only. They cannot be viewed or managed on the inactive Gateway. When a Gateway changes to the inactive state, it clears any Alerts that may have been active on that XRT.

- The XRT Gateway supports a “System Health Alert”. This alert is raised upon detection of certain conditions that may be detrimental to hardware or software performance. When the alert is raised, an Event Log entry is also created. The Event Log entry contains a “System Health issue number” that can be provided to Motorola Solutions technical support personnel for further investigation.

4.6.5 Automatic Fallback

The Connect Plus Auto Fallback feature allows the Connect Plus radio to automatically detect certain failure scenarios where the site repeaters are no longer communicating with the XRC Controller.

When the Control Channel repeater stops sending Connect Plus messages, the Connect Plus radio enters Search mode. If the radio detects that its configured Fallback Channel is operating in Fallback mode, the radio will stop searching and monitor its Fallback repeater. While operating on its Fallback Channel, the Connect Plus radio supports non-emergency Group voice call. This allows the radio to communicate with other subscribers that are currently monitoring the same repeater and timeslot and using the same Talk Group ID. All Call transmissions are also supported in Auto Fallback mode, and will be heard by all radios monitoring the same repeater and slot, regardless of which Group is currently selected on the receiving radio(s). Auto Fallback transmissions are not networked to other repeaters or sites.

Auto Fallback is not intended to be a long-term failure mitigation solution. Because Auto Fallback is designed to provide short-term, limited communications until the site can be repaired, it should be used to supplement (but not to replace) other failure preparedness strategies such as Redundant XRC and Redundant (i.e. multiple) Control Channels.

4.6.5.1 Failure Scenarios Supported by Auto Fallback

Auto Fallback is useful for the following failure scenarios:

1. Any controller failure that causes the controller to stop responding to Keep Alive messages from a repeater peer.

2. Any failure of site networking equipment (such as the LAN Ethernet switch) that causes the peer repeater to no longer receive Keep Alive responses from the controller.

3. Auto Fallback is useful for scenarios where the controller is still working, but it doesn’t have any useable Control Channel repeaters. Examples include the following:

   a. There is only one Control Channel on the controller Control Channel list, and that repeater is in error condition.

   b. There is more than one Control Channel on the controller Control Channel list, but all of those repeaters are in error condition.

Notes:
- “Error condition” means that the repeater has not checked-in with the controller, or that the repeater has reported one of the significant alarms that normally results in Control Channel Rollover. Interference on the Control Channel frequency does not trigger Auto Fallback operation.

- In certain rare scenarios (such as sudden failure of a single network cable), a single site repeater may enter Fallback mode of operation while other repeaters are still communicating with the XRC and operating normally. This condition can result in a split-fleet, with some radios monitoring a working Control Channel and other radios monitoring a Fallback Channel. In such a scenario, calls initiated on the Fallback Channel will not be heard by radios monitoring the Control Channel (and vice versa). The “isolated” repeater should be powered-down or disabled (if at all possible) until the condition is corrected.

4.6.5.2 Auto Fallback Overview

The following paragraphs provide a broad overview of how Auto Fallback works. It assumes that Auto Fallback is supported by all system software and that the feature has been enabled in both the subscriber radio and in the XRC controller. Additional details and configuration guidelines will be provided in subsequent sections.

There are several types of failure that can instigate Auto Fallback. The total time for a repeater to enter Auto Fallback mode can vary between one and two minutes, depending on the specific type of failure that instigates Auto Fallback. This is because there is always some period of time between the instigating failure and when the repeater detects loss of connectivity with the XRC. Once the repeater detects loss of connectivity with the XRC, it starts some internal timers. When these timers expire (after approximately one minute), and if there is still no connection to the XRC, the repeater enters conventional fallback operation and transmits a Connect Plus Fallback Beacon. The Fallback Beacon rides in a portion of digital signal that is common to both timeslots. So, it will be detected by a radio that is listening to either of the repeater’s timeslots (1 or 2).

When the repeater is repeating a call, the Fallback Beacon will be sent continuously. When the repeater is otherwise idle, it will transmit the Fallback Beacon at duration and interval set by the controller upon link establishment. Repeaters on the controller’s Control Channel (CC) list are instructed to send the Fallback Beacon continuously. Trunk Channel repeaters (non-CC repeaters) are instructed to send the Fallback Beacon at a duration and interval that is configured into the controller via the Network Manager. One of the configurable options is for continuous transmission.

The Connect Plus radio should be programmed with one Fallback channel for each site that supports Auto Fallback. After conducting normal Control Channel search for a period of time defined in Connect Plus CPS programming (and not having located any operable Connect Plus site), the Connect Plus radio will add a site's configured Fallback Channel to every site search.

The SU's Fallback repeater is one of the site's Control Channel or Trunk-to Channel Repeaters during normal operations. This means the repeater has multiple roles. When the site is operating normally, the repeater operates as a Control Channel repeater or as a trunk-to channel repeater. However, during certain failure scenarios, the repeater automatically becomes a Fallback repeater.

Fallback Channels fall into two categories; channels that transmit a continuous Fallback Beacon and channels that transmit a non-continuous (intermittent) Fallback Beacon. Channels that transmit a continuous Fallback Beacon can be located more quickly when the SU is searching. While any site repeater can be configured as the radio's Fallback Channel, only exclusively licensed Channels should transmit a continuous Fallback Beacon.

While searching a Fallback Channel, the length of time that the radio dwells on the frequency while listening for a Fallback Beacon is determined by Connect Plus CPS programming. Upon detecting its Fallback Channel, the Connect Plus radio remains on the Fallback channel and supports non-emergency Talk Group communications on the selected Talk Group ID (which includes the All Call ID, if so configured). The Connect Plus radio is also able to receive an All Call, even if it is not the selected Group ID. All other call features are not supported in Fallback mode.

When the radio is operating in Auto Fallback mode, it uses the same Talk Group IDs that is uses in Connect Plus trunking mode, and the radio user selects the desired Group in the same manner -- by selecting the Channel Knob (or Channel Rocker) position that is assigned to the Group.

Multiple Group IDs can share the same Fallback channel. For example, if some radios are selected to Talk Group "A" while other radios are selected to Talk Group "B", either Group can use the channel on a "first-come, first-served" basis. If Group A is using the channel, the Group A transmissions will not be heard by a radio that is selected to Group B. If the Group B user attempts to key-up during a Group A call, his/her radio operates politely. The radio plays the busy tone and displays "Channel Busy".

Group scan is not supported in Fallback mode. Therefore, a single radio in Fallback mode cannot simultaneously scan both Group A and Group B. However, it is possible to program both Groups into the radio. The radio user can then select the desired Group by changing the Channel Selector Knob (portable radio) or Channel Rocker (mobile).

The Connect Plus radio continues to use the Fallback channel until one following occurs: (a) the radio fades from the Fallback Channel and re-enters search, or (b) the site returns to normal Connect Plus trunking operation. When the site returns to normal Connect Plus trunking operation, the radio must perform a new registration with the site. After registering with the site, the radio can once again utilize its normal Connect Plus features.

4.6.5.3 Connect Plus CPS Settings for Auto Fallback

The next two sub-sections discuss the Connect Plus CPS settings for Auto Fallback. Prior to configuring these settings, it will be necessary to know some things about how the Fallback settings are configured in the site controller(s). The MOTOTRBO Connect Plus Network Manager is used to view and configure the Fallback settings in the site controller(s).

Configuring the SU's Fallback Channel with Connect Plus CPS

One of the most important decisions when configuring the SU for Auto Fallback is deciding which repeater and timeslot the SU should use for Auto Fallback operation at each network site. The Fallback Channel assignment is made using Connect Plus CPS. The XRC Controller and the Network Manager do not know which Fallback Channel the SU is assigned to. The term "Fallback Channel" includes both the Fallback repeater and the assigned timeslot on the Fallback repeater.

Consider the following when selecting the SU's Fallback Channel.

1. The SU can be configured for just one Fallback Channel per network site. If both the site controller and the configured Fallback repeater are out of service, the SU will not be able to use the site.

2. The Fallback Channel must be one of the repeaters that is normally used for Connect Plus trunking operations.

3. The repeater must have successfully checked-in with the XRC Controller prior to the failure that instigates Auto Fallback operation. During the check-in process, the controller gives the repeater the information it needs for Fallback operation, should this later become necessary. It is very important to note that the repeater does not maintain this information through a power cycle. Therefore, if the repeater loses power after (or in conjunction with) losing its connection to the XRC, the repeater will not send the Fallback Beacon, and it cannot be automatically detected by a Connect Plus radio.

4. Whether or not different radios can be configured to use different Fallback Channels at the same site depends on the following rules. These rules are not enforced by the system software, so the individual that configures the radios for Auto Fallback must enforce them. Failure to follow these rules will prevent Auto Fallback from operating as intended:

    a. Radios that share any common Talk Groups must be configured to use the same Fallback Channel at the same site. Radios share the same Fallback Channel when they are configured for both the same Fallback repeater and the same timeslot on that repeater. For example, Radio 1 is configured to use Talk Groups A, B, and C, and it is configured to use "Repeater 1, timeslot 1" as its Fallback Channel at Site 1. Radio 2 is configured to use Talk Groups C, D and E. Because these two radios share a common Talk Group (Group C), Radio 2 must also be configured to use "Repeater 1, timeslot 1" as its Fallback Channel at Site 1. If Radio 2 were configured to use any other Fallback Channel, this could result in a "split-fleet" scenario where some radios are using Group C on Repeater 1, timeslot 1 while other radios are simultaneously using the Group C on a different repeater (or the same repeater, but a different timeslot). Only the radios that are selected to the same Group ID and listening to the same repeater and timeslot will hear each other!

    b. Radios that do not share any common Talk Groups can be configured to use different Fallback Channels at the same site. For example, the radios for "Ted's Taxi" use Groups A-C. The radios for "Connie's Courier Service" use Groups D-E. These two companies never need to communicate with one another. Assigning these companies to two different Fallback Channels at the same site can help reduce the number of "busies" that are experienced by both companies by spreading the calls out over two Fallback Channels instead of one. For example, "Ted's Taxis" can be assigned to Repeater 1, timeslot 1 as their Fallback Channel while "Connie's Courier Service" is assigned to Repeater 1, timeslot 2 (or to any other repeater and slot) as their Fallback Channel.

5. Another important decision in selecting the SU's Fallback Channel is whether the channel can be configured to send a "continuous" Fallback Beacon or not. (This is configured via Network Manager programming, as discussed in a later paragraph). Channels that send a continuous Fallback Beacon can be searched more quickly than channels that send a non-continuous (intermittent) Fallback Beacon. The continuous Beacon especially helps when the radio has to search through several sites prior to locating a Fallback Channel. The cumulative effect of the shorter search times can be significant. It is important to

remember that a repeater should not be configured to send a continuous Fallback Beacon unless it has a Protected Service Area. Non-exclusive licenses such as FB2 or FB6 are not suitable for continuous Fallback Beacons, just as they are not suitable for Connect Plus Control Channels.

6. Because it is desirable to send a continuous Fallback Beacon on a radio's Fallback Channel, most customers will utilize the site's Control Channel frequency (or frequencies) as the Fallback frequency (or frequencies). This is permitted. When the repeater is connected to the XRC, it will operate as a Connect Plus Control Channel repeater (or trunk channel repeater, if another Control Channel repeater is currently active). However, when the repeater loses connectivity to the XRC for a period of time, it will start sending a continuous Fallback Beacon.

7. It is also allowable to use a repeater that is not on the Control Channel list as a Fallback Channel. This is most desirable for customers that have the luxury of a protected service area (i.e. an exclusive license) for all site repeaters. If using a co-licensed channel for the Auto Fallback Channel, it is critical to remember the following:

    a. The repeater should not be configured with the Network Manager to send a continuous Fallback Beacon. It should be configured to send a non-continuous (intermittent) Fallback Beacon.

    b. When the co-licensed user is using the frequency, the repeater is required to temporarily disable itself to comply with FCC Type 1 and Type 2 regulations for co-licensed channels. During the period that the co-licensed user is utilizing the frequency, the repeater cannot transmit the Connect Plus Auto Fallback Beacon. If the repeater does not transmit the Fallback Beacon for an extended period of time, the Connect Plus radios will leave the Fallback Channel and re-enter Search mode.

8. Use Connect Plus CPS to configure a Fallback Channel list for each Network ID that will be utilized by the SU. For each supported Network ID, configure one Fallback Channel per site. The required information for configuring a Fallback Channel is as follows:

    a. Check the "Fallback Channel" box for each network site that has a Fallback Channel.

    b. Enter the (SU's) Transmit Frequency

    c. Enter the (SU's) Receive Frequency

    d. Configure the timeslot to use for Fallback operation (1 or 2)

    e. Enter the repeater's Color Code

    f. Continuous Beacon checkbox: Check the box if this repeater is on the site's Control Channel list in the site controller. If the repeater is not on the site's Control Channel list in the site controller, then it will be necessary to check the configuration of the parameter called "Non-CC Repeater Settings: Beacon Interval" in the site controller:

        i. If "Non-CC Repeater Settings: Beacon Interval" is set to zero, then check the CP CPS box labeled "Continuous Beacon"

        ii. If "Non-CC Repeater Settings: Beacon Interval" is set to a value greater than zero, then do not check the CP CPS box labeled "Continuous Beacon". This tells the Connect Plus radio that the channel will be sending a non-continuous (intermittent) Fallback Beacon.

Note: If a site has just one Control Channel repeater, it is recommended to use a different site repeater as the SU's Fallback Channel. This provides a crude form of Control Channel Backup for scenarios where the site's only Control Channel repeater fails, but the site controller is still operative. If a site has multiple Control Channel

repeaters, it is acceptable to use one of these repeaters as a Fallback Channel, since it is desirable to send a continuous Fallback Beacon whenever possible.

Configuring other Fallback Settings with Connect Plus CPS

On the General Zone Parameters screen, Connect Plus CPS contains three important settings that are configurable per Connect Plus zone.

Enable Fallback Search
When this checkbox is disabled (unchecked), the Connect Plus radio will only search for operable Connect Plus Control Channels while selected to this Connect Plus zone. If the Connect Plus radio detects a Fallback Beacon while searching for a Control Channel, it will not stop on the Fallback Channel. It will continue to search for an operable Connect Plus Control Channel.

When this checkbox is enabled (checked), the Connect Plus radio will begin inserting Fallback Channels into its Search routine when the timer value defined in “Begin search Fallback Channels after ‘n’ seconds” has expired; (n = configured value in seconds).

Begin Searching Fallback Channels after n seconds (n = configured value in seconds)
When the Connect Plus radio starts Searching for service, it starts this timer. Prior to expiration of the timer, the radio searches only Connect Plus Control Channels. If the timer expires, and if the radio is still Searching, the radio begins adding the site’s Fallback Channel to the search routine (after first searching the site’s Control Channels).

The configurable range is 10 to 60 seconds. Setting the timer towards the lower end of the range can help the Connect Plus radio to locate a Fallback Channel more quickly, but it also slows down the Search process for normal conditions. By “normal conditions”, this means that all sites are working properly (no Fallback Channels active), and the radio should continue searching Control Channels until it locates a site that is within range.

The following example shows how the Connect Plus radio search order is impacted by this setting:

Sample search order prior to expiration of “Begin Searching Fallback Channels after “n” seconds:
- Site 1 Control Channel #1
- Site 1 Control Channel #2 (if configured)
- Site 1 Control Channel #3 (if configured)
- Site 1 Control Channel #4 (if configured)
- Site 2 Control Channel #1
- Site 2 Control Channel #2 (if configured)
- Site 2 Control Channel #3 (if configured)
- Site 2 Control Channel #4 (if configured)
- Etc.

Sample search order after “Begin Searching Fallback Channels after “n” seconds” expires:
- Site 1 Control Channel #1
- Site 1 Control Channel #2 (if configured)
- Site 1 Control Channel #3 (if configured)
- Site 1 Control Channel #4 (if configured)
- Site 1 Fallback Channel, if configured
- Site 2 Control Channel #1
- Site 2 Control Channel #2 (if configured)
- Site 2 Control Channel #3 (if configured)
- Site 2 Control Channel #4 (if configured)
- Site 2 Fallback Channel, if configured
- Etc.

Note: When the Connect Plus radio is enabled for Fallback operation, it starts this timer whenever it enters Search. This includes scenarios where the radio has been using a Fallback Channel, and then enters Search because it has not decoded the Fallback Beacon within an expected period of time, or because the radio user has pressed the Roam Request button. The radio only searches only Control Channels until this timer expires.

It should also be noted that the Connect Plus radio can detect a Fallback Beacon before this timer expires. This is because Control Channels can also be configured as Fallback Channels. If the Connect Plus radio is Searching a Control Channel, and if it detects a Fallback Beacon, and if this channel is the radio's configured Fallback Channel for the site, the radio will stop its search and utilize the channel in Fallback mode, even if this timer has not yet expired.

Dwell time for non-continuous Beacon
When the radio is searching a Fallback Channel that is not flagged for "Continuous Beacon" on its Fallback Channel list, the Connect Plus radio "dwells" for this amount of time as it listens for a Fallback Beacon. If no Fallback Beacon is detected within this period of time, the radio moves on to the next channel in its search list.

- If all Fallback Channels send a Continuous Beacon, then this setting isn't used. In that case, the recommendation is to leave the setting at its default value.

- If any Fallback Channel sends a non-Continuous (intermittent) Beacon, then this setting must be configured to match the value that is configured for the setting called "Non-CC Repeater Settings: Beacon Interval" in the site controller(s). The one exception is when Beacon Interval is set to 0 seconds in the site controller(s). In that case, set the "Dwell Time for non-continuous Beacon" to 1 second in Connect Plus CPS.

This setting determines the Dwell time for Fallback Channels that are not flagged as "Continuous Beacon" channels. For Fallback Channels that are flagged as "Continuous Beacon" channels, the Connect Plus radio uses the same "Roam Dwell Time" that it uses when searching Connect Plus Control Channels. (This is because Connect Plus Control Channels also transmit continuously). That timer is configured under "Roaming and Search Settings" on the Connect Plus CPS General Zone Parameters screen.

Configuring the Controller's Automatic Fallback Settings with the Network Manager

Use the MOTOTRBO Connect Plus Network Manager to view/configure the Automatic Fallback settings in the site controller(s). The settings are located on the Configuration screen (*Settings → Configuration*), in the "Critical Settings" panel. Changes to the Automatic Fallback settings require an XRC Reboot to take effect.

Enable Fallback Beacon (checkbox)
When enabled (checked), the XRC commands every repeater that checks in with this controller to send a Connect Plus Fallback Beacon if the repeater should lose its connection to the controller for a period of time (approximately one minute).

- Repeaters on the Control Channel list are instructed to send a continuous Fallback Beacon. The system software makes the following assumption; any channel that is suitable for Control Channel operation (and placed on the Network Manager's Control Channel list) is also suitable for sending a continuous Fallback Beacon.

- Repeaters that are not on the Control Channel list are instructed to send a Fallback Beacon at the Interval and Duration defined under, "Non-CC Repeater Settings".

When disabled, the XRC does not command any repeater to transmit a Connect Plus Fallback Beacon. When a repeater checks in, the controller sends a command to disable Fallback functionality in the repeater.

Note: It is important to emphasize that when Automatic Fallback is enabled in the controller, every repeater will transmit the Fallback Beacon after losing connectivity with the controller for a period of time. However, this does

NOT mean that every repeater will be used as a Fallback Channel by subscriber units. It is possible that every SU may be programmed to use the same Fallback Channel, or different SU's may be programmed to use different Fallback Channels. This information is configured into the SU with Connect Plus CPS. The Network Manager and the XRC do not know how the radio has been programmed.

Additionally, if the repeater version is lower than 1.9A the Connect Plus Fallback Beacon is not transmitted. In this case, when the controller's **Enable Fallback Beacon** option is on, the subscriber units can still manually switch to conventional radio personality (defined in non-Connect Plus zone) and operate in conventional mode.

Non-CC Repeater Settings: Beacon Interval

When Automatic Fallback is enabled, this setting determines how long that any repeater not on the Control Channel list will rest between transmit cycles when sending the Fallback Beacon (assuming that the repeater is otherwise idle and not repeating any call). The configurable range is 0 to 30, in increments of 1 second. A setting of 0 (zero) tells the repeater to transmit the Fallback Beacon continuously. While a setting of 0 (zero) achieves the fastest possible Search times for the Connect Plus radio, it should only be used for repeaters with a protected service area. It should not be used when the repeater frequency has a non-exclusive license such as FB2 or FB6.

If any Connect Plus radio is configured to use a Non-Control Channel repeater as its Fallback Channel, and if the repeater is configured with a Beacon interval greater than zero, then use the following rule for configuring the radio's setting for "Dwell time for non-continuous Fallback Beacon":

- The Dwell Time for non-continuous Beacon configured with Connect Plus CPS should be set to the same value as "Non-CC Repeater Settings Beacon Interval" configured with the Network Manager. The one exception is when Beacon Interval is set to 0 seconds in with the Network Manager. In that case, set the "Dwell Time for non-continuous Beacon" to 1 second in Connect Plus CPS programming.

Configuration Tip: If the Connect Plus radios are configured to only search Control Channel frequencies as Fallback Channels, then set "Non-CC Repeater Settings" Beacon Interval" to its greatest possible value (30 seconds) and "Non-CC Repeater Settings" Beacon Duration" to its shortest possible value (480 ms).

Non-CC Repeater Settings: Beacon Duration

When an idle non-Control Channel repeater transmits the Fallback Beacon, it shall transmit the Beacon for this duration before resting its transmitter. Once the repeater has rested for the duration defined in Beacon Interval, the repeater transmits the Beacon once again for the Beacon Duration. This process repeats in a cycle as long as the repeater remains idle. The programmable range is 480 ms to 18000 ms in increments of 120ms. When the Beacon Interval (see previous section) is set to zero (i.e. continuous), the duration is not significant. Setting the Beacon Duration to the higher end of the programmable range increases the chances for a Searching radio to detect the Fallback Beacon. However, it also creates more "wear and tear" on the repeater and provides a smaller window of opportunity for co-licensed users to utilize the frequency.

Connect Plus Fallback Beacon

The Fallback Beacon plays an integral role in the Auto Fallback feature.

1. In order for the repeater to transmit a Fallback Beacon, all of the following must be true:

   a. The repeater software must be MOTOTRBO Release 1.9A, or higher.

   b. The repeater must check-in with the site controller at a time when the controller is operative.

   c. Prior to the repeater check-in, Automatic Fallback must have been enabled in the site controller with the MOTOTRBO Connect Plus Network Manager.

   d. The repeater must not have experienced a reset or power cycle since its most recent check-in with the site controller.

2. Assuming that all of the above are true, the repeater begins to transmit the Connect Plus Fallback Beacon after losing connectivity with the XRC for a period of time (approximately one minute).

    a. During the period of the time that the site is transmitting neither Control Channel messages nor the Fallback Beacon, the Connect Plus radios will start Searching for service. If there is overlapping site coverage, this will cause some radios to register with a different Connect Plus site.

    b. When the repeater is repeating a call on either timeslot, it transmits the Fallback Beacon continuously in the portion of the digital signal that is common to both timeslots.

    c. When the repeater is not repeating a call (the repeater is idle), it transmits the Fallback Beacon at the Interval and Duration instructed by the controller when the repeater checked-in with the controller. The controller sets the Interval and Duration as discussed in the sub-section, “Configuring the Controller’s Fallback Settings with the Network Manager.”

    d. The repeater(s) can be expected to briefly send the Fallback Beacon after “voluntary resets” of the XRC Controller. This may cause the site radios to briefly enter Fallback mode. A “voluntary reset” occurs when the Network Manager user issues the reboot command, after updating certain Critical settings with the Network Manager, and following an XRC Firmware Upgrade. Once the XRC has rebooted and re-established communications with the repeaters, the Connect Plus system will return to normal operation.

3. When the Connect Plus radio is searching for service, the Fallback Beacon tells the radio that it has detected a repeater that is operating in Fallback mode.

4. The Fallback Beacon conveys both the Network ID and the Site Number. The Connect Plus radio will not stop and utilize the Fallback Channel unless all of the following are true:

    a. The Network ID matches the Network ID that is configured for the currently selected Connect Plus zone.

    b. The Site Number is an allowed site for the indicated network. (Note: The site is considered to be allowed unless the site controller informs the SU that the site is disallowed before the site enters Fallback mode.)

    c. The frequency and Color Code match the SU’s configured Fallback Channel info for the indicated Network and Site.

5. It is important to note that the presence of the Fallback Beacon does not prevent the radio from making a call. This is because the Beacon rides in the portion of the digital signal that is between timeslots.

6. After the Connect Plus radio has acquired a Fallback Channel (based on the presence of the Fallback Beacon), the radio must continue to periodically decode the Fallback Beacon in order to continue using the Fallback Channel. This assures the radio that it has not faded from the coverage of the Fallback repeater (or into the coverage of a different repeater). If the radio cannot periodically verify that is still receiving the Fallback Beacon, the radio will re-enter Search mode.

7. The Connect Plus radio acquires (and remains on) a Fallback Channel based on the presence of the decoded Fallback Beacon. The Connect Plus radio does not qualify the RSSI of a Fallback Channel. This is because Fallback Channels are not required by rule to transmit continuously (although this is desirable, whenever possible).

8. When the site returns to normal trunking operation, the repeater stops sending the Fallback Beacon. After re-establishing its connection to the controller, the system sends a message to tell the SU that the channel has returned to Connect Plus trunking mode. When the Connect Plus radio decodes this

message, it will search for the site's active Control Channel and, upon detecting the Control Channel, sends a Registration Request to the site controller.

4.6.5.4 Operating on the Fallback Channel

The section outlines how the Connect Plus radio operates after acquiring its Fallback Channel:

1. While the Connect Plus radio is operating on a Fallback Channel, it plays a short tone approximately every 15 seconds (except while transmitting). The tone notifies the radio user that the radio is operating in Fallback mode and has a limited feature set. (Note: The Fallback tone is not played if the "Disable all tones" box is checked on the Connect Plus CPS General Settings screen.) In addition to the Fallback tone, display-equipped models periodically show the message, "Fallback Channel".

2. While operating on a Fallback Channel, the Connect Plus radio will unmute to non-Emergency voice calls on its selected Group ID and the All Call ID.

3. The Connect Plus radio allows the radio user to transmit on the currently selected Group ID if the Fallback Channel is idle, or if there is an ongoing call for the same Group, and the call is in Group Hang Time. If the channel is currently busy when the radio user presses PTT, the radio sounds the Busy Tone and displays "Channel Busy". (Note: Multiple Group IDs might be sharing the same Fallback Channel. Because the radio only unmutes for the Selected Group ID and the All Call ID, the radio user might not be aware that the channel is busy prior to pressing PTT.)

4. If the radio's Multigroup ID is the currently selected Group ID, this operates just like any other Group ID while in Fallback mode. Other radios will not unmute to the transmission unless they are selected to the Multigroup ID also.

5. The Talk Group assignments that are configured via the Contact Name field on the Connect Plus Zone Channel Selections screen determine which Group is assigned to which Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio). These Group assignments apply to Connect Plus trunking mode and to Fallback mode. The radio user can change to a different Group by selecting a different position on the Channel Selector Knob or Channel Rocker, if the radio is so programmed with Connect Plus CPS.

6. If a Private Call Contact is assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio), this is not supported in Fallback mode. If the radio user selects this Channel Selector Knob or Channel Rocker position (while operating on a Fallback Channel), and then presses PTT to initiate a call, the radio will play a PTT denial tone. The radio user should select a different position that is assigned to a Group Contact.

7. Fallback Mode supports non-emergency Group Calls (including the All Call ID) only. All other call types are NOT supported in Fallback Mode. If the radio user should attempt to initiate any non-supported call type, the radio will provide an invalid key press tone and display-equipped models will also show a brief failure message.

8. Calls are heard only by radios that are monitoring the same Fallback Channel repeater and selected to the same Talk Group ID. Calls are not networked to other sites or other repeaters.

9. The Enhanced Privacy feature is available while operating in Fallback mode.

10. The RX Only feature (which is configured on the Connect Plus Channel Selections Screen) is supported while operating in Fallback mode. If the selected Group is configured as "RX Only", the radio can receive calls on the Group, but cannot transmit.

11. Enhanced Traffic Channel Access (ETCA) is not supported in Auto Fallback mode. If two or more radio users press PTT at the same time (or at almost the same time) while operating on the Fallback Channel, it is possible that both radios will transmit until PTT is released. In this event, it is possible that none of the transmissions will be understood by receiving radios.

Base Station Identification (BSI) on Fallback Repeaters

When the repeater is operating in Fallback Mode, it periodically sends Base Station Identification (also known as CWID) at the TX Interval configured into the repeater codeplug with MOTOTRBO CPS. (During Fallback operation, the repeater does not use the BSI Interval configured with the MOTOTRBO Connect Plus Network Manager.)

If the repeater is configured for analog BSI, when the repeater sends BSI, it transitions to analog mode to send the Morse Code characters configured into the (CWID) ID field with MOTOTRBO CPS. During this time, the repeater does not transmit the Fallback Beacon. If a Connect Plus radio happens to be searching the frequency during the ID (in other words, the radio has not yet acquired the channel), it will not detect any digital signaling and will move to the next frequency on its Search list.

If a Connect Plus radio has previously acquired the Fallback Channel, and then the repeater transitions to analog mode to transmit its CWID, the radio will not detect any digital activity from the repeater for the duration of the CWID. In order to prevent the Connect Plus radio from roaming away from the repeater during CWID, configure the Connect Plus radio per the following rule:

- MOTOTRBO Connect Plus CPS provides a configurable setting called, “BSI Wait Time” per Connect Plus zone. Set the BSI Wait Time to the “worst case” length of time required to send the Morse Code identification for any Control Channel repeater or Fallback repeater that will be used by the SU in the selected network, plus an extra 5 seconds to allow adequate time for the digital-analog and analog-digital transitions.

It should be noted that the BSI Wait Time also helps determine how quickly the Connect Plus radio will roam away from a Fallback Channel during a normal fade condition.

Call Hang Time values used by repeater

When the repeater is operating in Connect Plus mode (as a Connect Plus Control Channel or trunk-to channel repeater), the repeater utilizes the Group Call Hang Time, Private Call Hang Time, and Emergency Call Hang Time values configured into the XRC Controller with the MOTOTRBO Connect Plus Network Manager. The XRC sets the repeater’s SIT timer behind-the-scenes, based on the values configured for the call hang timers.

When the repeater is operating in Auto Fallback mode, the repeater utilizes the Group Call Hang Time and Subscriber Inactivity Time (SIT) values configured with MOTOTRBO CPS. Private Call Hang Time and Emergency Call Hang Time do not apply to Fallback mode, since these call types are not supported during Fallback operation.

Interaction of Auto Fallback and Emergency features

⚠ **IMPORTANT!** Emergency Call and Emergency Alert are not supported in Fallback mode!

- If the radio user should attempt to press the Emergency button while the Connect Plus radio is operating on a Fallback Channel, the radio will provide an invalid key press tone and display-equipped models will also show a brief failure message.

- If the radio is searching for service with Emergency Pending, and if the radio detects a Fallback Beacon while searching, and if Fallback Search has been enabled with Connect Plus CPS, and if the Fallback Beacon is being transmitted by the radio's configured Fallback Channel for that site and network, the Connect Plus radio will stop on the Fallback Channel and automatically cancel the user's emergency! The user receives no indication that this has occurred, other than hearing the periodic Fallback tone that the radio plays after acquiring a Fallback Channel.

Interaction of Auto Fallback and Connect Plus Man Down features

The Connect Plus radio automatically cancels all timers, tones, and operation associated with the Man Down feature (if active) upon acquiring a Fallback Channel. It will not restart any timers, tones or operation associated with the Man Down feature as long as the radio remains on the Fallback Channel.

Testing Auto Fallback Configuration

As with other features, it is important to test Auto Fallback operation to assure that the Connect Plus radios and site controllers have been configured correctly. However, testing the system's Auto Fallback configuration presents some special challenges. In order to test Fallback operation, it will be necessary to remove the site from normal Connect Plus trunking operation for a period of time. This should preferably be done during a low-use time (such as the middle of the night, for example). Any radio users that are using the site(s) when the Fallback feature is tested should be notified of what to expect prior to starting the test. During the test, their radios will have limited functionality.

Once all settings have been configured in both the subscriber radios and the XRC controller(s), the recommended method to initiate Auto Fallback is as follows:

1. Connect to the desired site (which should be currently operating in normal trunking mode) with the MOTOTRBO Connect Plus Network Manager.

2. After connecting, select *Settings→Configuration*, and locate the "*Repeaters On*" checkbox in the Critical Settings section. Uncheck the box, and then press "*Save*".

3. This causes the XRC to reset. After rebooting, the XRC will not accept any check-ins from the site repeaters.

When the controller resets (as described in the previous paragraph), radios that were listening to the site will go into Search. If the site has overlapping coverage with other network sites, some of the radios may change sites. This is to be expected. The repeaters will start to send the Fallback Beacon approximately one minute after losing their connection to the XRC. Radios that have not acquired another site should eventually locate and monitor their Fallback Channel. After the radio finds its Fallback Channel, the radio user can make a non-emergency Group Call on the selected Group Contact. Radios that are using the same Fallback Channel and selected to the same Group Contact should be able to communicate.

When you are ready to conclude the test, repeat the steps above, except this time check the "*Repeaters On*" checkbox, and press "*Save*". Once again, the XRC will reboot. After the reset, the controller will begin accepting check-ins from the site repeaters. Operation will return to normal when all repeaters have finished checking-in with the active XRC and when the radios have re-registered with the site.

4.6.6 Mitigating Mass Registration Scenarios

During mass registration scenarios, when hundreds of subscribers attempt to register simultaneously on a Connect Plus site, there is high occurrence of RF collisions on the Control Channel inbound link. In such cases, multiple transmissions collide over the air resulting in delayed voice communications and data services for the end users. The following paragraphs provide recommendations on mitigating mass registration conditions by reducing the RF contention.

One of the codeplug parameters in the Connect Plus Option Board is called **Reacquire Timer**. When the radio loses acceptable signal from its current site and begins searching, a countdown timer is set to this value. If during the search process the radio again finds the site it just lost, and this timer has not expired and the radio has not attempted to register at another site, the radio returns to the registered state without transmitting a registration request to the site.

Adjusting the Reacquire Timer can help reduce registration traffic on the control channel. The timer default value is set to **30 seconds**. When the Connect Plus system has a single site, it may make sense to set this timer out to a longer period of time for critical Talk Groups. The maximum amount the timer can be set to is **600 seconds** (10 minutes) before the subscribers need to register again to the same site. The Reacquire Timer could be one adjustment that is used to allow the subscribers to keep looking for the site longer, prior to having to re-register to that site.

This parameter is useful in cases of Control Channel repeaters outage that is shorter than 10 minutes (longest Reacquire Timer that can be provisioned in the Option Board). Before performing the site maintenance requiring Control Channel outage, it is highly recommended to utilize the **Site All Call** feature and announce the planned outage multiple times[46] to inform the users of upcoming loss of service and the expected maintenance duration.

Note: In cases when a planned or unplanned controller reboot occurs, all the subscribers would attempt to register to the site once again; therefore, mass registration is unavoidable.

If a planned or unplanned outage involves a controller reboot, or if the outage lasts longer than the **Reacquire Timer**, it may be best to implement some of the following procedures for the subscribers:

- Train users to **not** change the channel knob (Talk Groups) during an outage. This causes the subscribers to re-register to the system every time the knob is changed. This causes excessive registration requests on the control channel and increases the probability of RF collisions.
- Talk Groups that are non-critical should power down after the reacquire timer has expired. After a specified amount of time, by Talk Group the users should power down the radios to minimize RF collisions on the control channel once it returns.
- Talk Groups that are critical, such as Emergency Services, Management, and Operations should remain on the air while the system is down. Once the Control Channel comes back these will be the first users to register back onto the system.
- Once the critical Talk Groups have registered back onto the system, continue contacting other talk groups to power up and register back onto the system a Talk Group at a time (in a controlled manner). Continue this process, until the full subscriber base is back onto the system.

When the Auto Fallback feature is enabled and if the site starts operating in Auto Fallback mode, unless the radios roam to another site, they will land on the corresponding Fallback Channels as configured in their Option Board codeplugs. Subsequently, when the Control Channel is restored the radios will switch to Connect Plus trunking mode and would attempt to register to the site once again; therefore, mass registration is unavoidable in this case.

[46] Since some users might be participating in calls during the initial announcement, issuing multiple announcements ensures that most users will hear at least one of the warnings.

Finally, to avoid Control Channel loss it is highly recommended to utilize the Connect Plus redundancy features as described in section "Connect Plus Failure Preparedness".
Beginning with MOTOTRBO Release 1.7 (R2.6.0), the Connect Plus system provides the following enhancements to assist with Mass Registration Collision Mitigation.

- Depending on device model and firmware level, some repeaters can automatically detect some types of message collisions on the Control Channel input frequency and notify the controller that collisions are being detected. The controller then uses outbound repeater messaging to request that registering radios extend their retry timers until the collisions are no longer detected at the same rate. No special configuration is required to enable this feature when supported by the repeater.

- The controller has a configurable setting called "Raise Access Level On Boot". Enable this setting if a large number of radios typically re-register with this site controller after device reboot. When enabled, the controller uses outbound repeater messaging to request that registering radios extend their retry timers for at least one minute following boot. This setting is useful for a single site deployment with a large number of subscriber radios. It is also useful for multisite deployments when the site that is being configured does not have adjacent sites with overlapping coverage.

4.6.7 XRT Redundant Gateway

The XRT Gateway is an optional component of the MOTOTRBO Connect Plus digital trunking system that allows connectivity from authorized clients that are part of the Motorola Solutions Application Development Partner (ADP) Program. For information on the XRT Gateway and its features, see section 3.1.1.5.

The customer can purchase a second XRT Gateway to serve as backup to the primary XRT. The Primary Gateway can be either a XRT 9000 or a XRT 9100. The Secondary Gateway can also be either a XRT 9000 or a XRT 9100. For both Gateways, the Talk Path licenses **must match** (the number of licensed Talk Paths must be equal).

In the event of Primary XRT failure, the Secondary XRT will take over operations automatically and be ready to process Client authentication and Talk Path registration within one minute. From the time the Primary XRT fails until the Client re-establishes connections and registers Talk Paths with the Secondary XRT, the customer experiences an interruption of service. However, recovery of service is automatic and requires no user intervention.

This feature allows the XRT to continue functioning after one failure by supporting automatic switchover from the Primary Gateway to the Secondary Gateway. However, the feature does not protect against multiple simultaneous failures, and it does not support automatic switchover from the Secondary Gateway back to the Primary. The XRT Configuration Tool user must request switchover from Secondary to Primary when he/she is confident that the reason for the original failure has been identified and corrected.

There are some pre-requisites for utilizing the Redundant Gateway feature:

1. A single Connect Plus network supports up to five XRT Gateways. For each XRT where redundant operation is desired, the customer must purchase a second XRT Gateway. The instructions in this section should be repeated for each XRT where redundancy is desired.

2. The Redundant Gateway set-up requires a total of three Ethernet cables to plug into Ethernet ports on the XRT Gateways. Standard Ethernet cables are used to connect the port labeled LAN1 on each Gateway to the site's Ethernet Switch. The third cable is used to directly connect the two ports labeled LAN2 on each Gateway. An Ethernet cross-over cable is required for the direct connection.

3. The XRT Client(s) must support Redundant XRT operation:

   a. The XRT Client(s) must detect the failure of network communications with the Primary XRT and must re-establish communications with the Secondary XRT, including authentication and Talk Path registrations.

   b. XRT Airtime Clients must re-connect, re-authenticate, and re-request the Airtime feature.

   c. The XRT Client(s) must make any other adjustment(s) that may be necessary for its internal audio routing and/or communication with other components of the Client’s hardware or software.

Note: The Client reconnects to the Primary XRT LAN1 IP address and is unaware that it is connecting to a different device. The Client application must re-connect after detecting the disconnection of the network TCP/IP socket used for the previous connection, or by cessation of heartbeat messages.

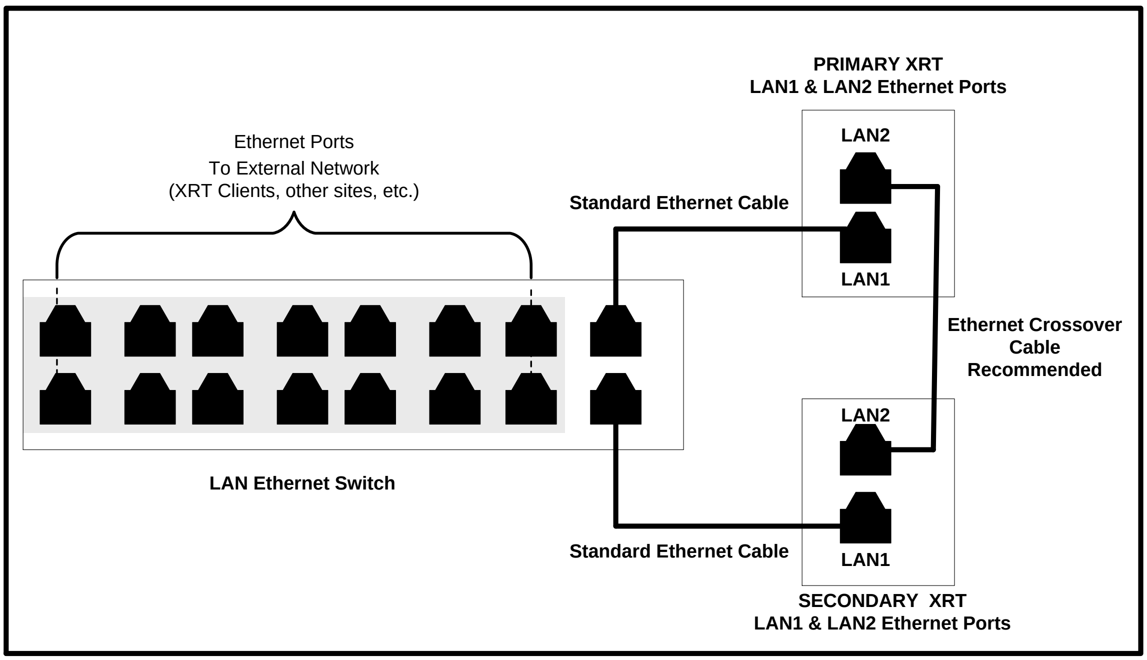


Figure 4-12 Redundant XRT: Ethernet Cable Connections

4. Except for their different roles (one configured as “Primary” and the other as “Secondary”), the two Gateways require the same configuration and user information to start with. The Network Settings must be configured separately for each Gateway. Other settings will be automatically shared when the Primary and Secondary Gateways are connected together and automatically synchronize certain information.

5. The Network Settings screen requires a total of 4 static IP addresses (two for each Gateway), as depicted in Figure 4-13 and discussed in Table 4-7.

6. It is highly recommended that the Secondary XRT Gateway should be licensed for the same number of Talk/Data Paths as the Primary XRT Gateway. If the Primary XRT Gateway utilizes the XRT 9100 hardware platform while the Secondary XRT Gateway utilizes the XRT 9000 hardware platform, it may not be possible to license the two devices for the same number of Talk/Data Paths. In this event, when the Secondary XRT Gateway takes over operation, it will support the XRT Client operations according to the capability of the XRT 9000 platform. The XRT Client application’s Talk/Data Path registration and call capability may be reduced after automatic failover.

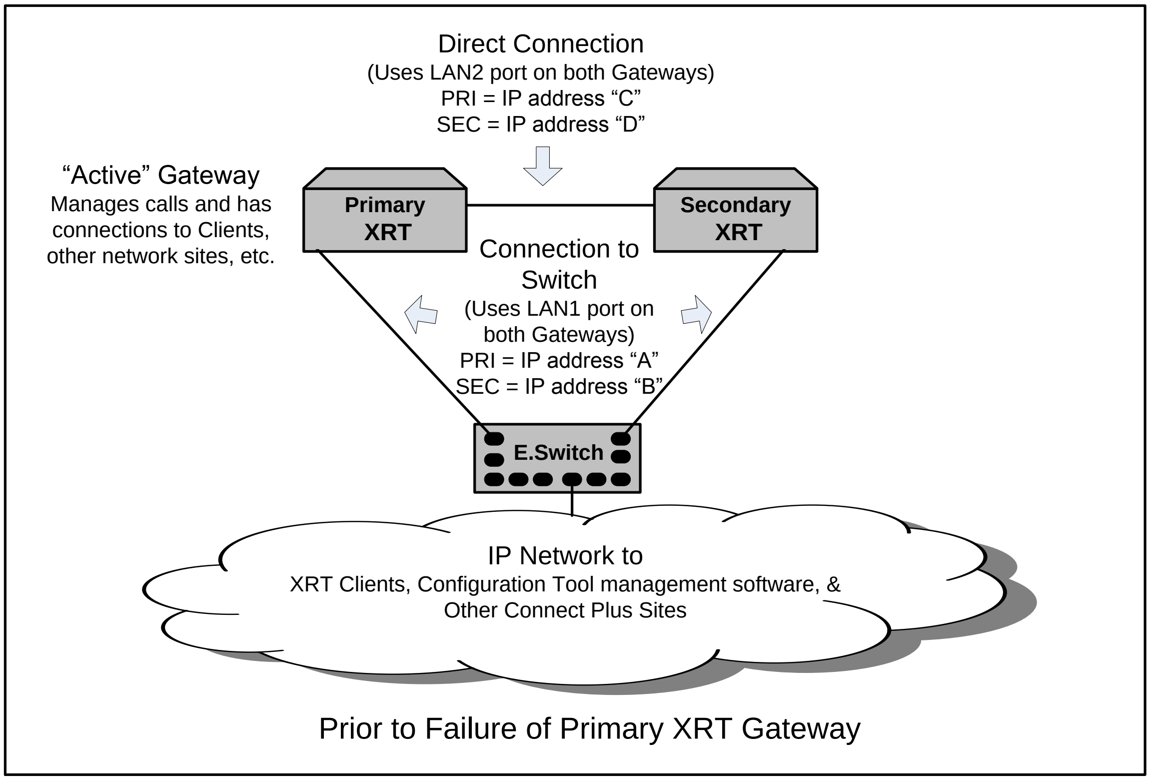


Figure 4-13 Redundant Gateway Configuration with Primary XRT Active

IP Address "A" (Static IP address)	• Configured as "Primary" (LAN1) IP Address • Used to address the Gateway that is currently "active", regardless of whether it is the Primary or Secondary. • IP address configured into the XRT Clients • Multisite Tables of other Connect Plus sites point to this address • Configured "Network Properties" apply to this address
IP Address "B" (Static IP address)	• Configured as "Secondary" (LAN1) IP Address • Used to address the Gateway that is currently "inactive", regardless of whether it is the Secondary or Primary • Configured "Network Properties" apply to this address
IP Address "C" (Static IP address)	• Configured as "Primary" (LAN2) IP Address • Used only for the direct connection between the two XRT Gateways. Only the two Gateways know about this address. • Always belongs to the Primary Gateway, regardless of whether it is "active" or "inactive" • First three octets of this address must be exactly the same as first three octets of IP address "D" (Secondary [LAN2] IP address). • First three octets of this address must be different than the first three octets of IP Address "A" and IP Address "B". • Configured "Network Properties" do not apply to this address
IP Address "D" (Static IP	• Configured as "Secondary" (LAN2) IP Address • Used only for the direct connection between the two XRT Gateways. Only the two Gateways know about this address.

address)	• First three octets of this address must be exactly the same as first three octets of IP address “C” (Primary [LAN2] IP address). • First three octets of this address must be different than the first three octets of IP Address “A” and IP Address “B”. • Configured “Network Properties” do not apply to this address
Notes:	• The Primary & Secondary Gateways can automatically “swap” Addresses A & B in switchover scenarios, but the XRT Configuration Tool configuration remains the same. • The Primary & Secondary never “swap” Addresses C & D

Table 4-7 XRT Gateway IP Addresses

Basic Concepts

Gateway Roles that can be configured in the XRT Configuration Tool software

Every XRT has one of three “roles” as discussed below:

- **Stand-alone**: This is the role of a Gateway that doesn’t have any redundant backup. It is the default Gateway role, and will not change unless the XRT Configuration Tool is used to configure a different role.

- **Primary**: This is the role assigned to the Gateway that should be in charge during normal operation. Once assigned the Primary role via the XRT Configuration Tool, it is always referred to as the Primary Gateway – even if the Secondary Gateway detects a fault and takes over.

- **Secondary**: This is the role assigned to the Gateway that should be in “stand by” during normal operation. Once assigned the Secondary role via the XRT Configuration Tool, it is always referred to as the Secondary Gateway – even if it takes over control.

Non-configurable states

In conjunction with the configurable roles, there are two important non-configurable states:

- **Active Gateway**: This is the Gateway currently in control (Clients, calls, etc.), regardless of whether it is the Primary or Secondary.

- **Inactive Gateway**: This is the Gateway currently not in control (Clients, calls, etc.), regardless of whether it is the Secondary or Primary.

    - While the Secondary Gateway is inactive, it is usually (if configured & connected correctly) in “standby” mode – ready to take over control if there is a failure of the Primary Gateway.

    - While the Primary Gateway is inactive, it is not in “standby” mode. It will not automatically switch back to being the active Gateway. For switch back to occur, the “Switch to Primary” command must be sent using the XRT Configuration Tool software.

Connecting with the XRT Configuration Tool

1. When connecting to the active XRT, enter the Primary LAN1 IP address (IP Address “A” in the preceding table) in the “Host” field on the XRT Connection Screen. The XRT Configuration Tool uses this address for communicating with the active Gateway (i.e. current handling Client connections and calls). This could be either the Primary or Secondary Gateway. The XRT Configuration Tool status bar will show whether the XRT Configuration Tool connects to the Primary or Secondary Gateway via this IP address.

2. When connecting to the inactive XRT, enter the Secondary LAN1 IP address (IP Address “B” in the preceding table) in the “Host” field on the XRT Connection Screen. The XRT Configuration Tool uses this address for communicating with the inactive Gateway. This could be either the Primary or Secondary Gateway. The XRT Configuration Tool status bar will show whether the XRT Configuration Tool connects to the Primary or Secondary Gateway via this IP address.

3. Do **not** use the XRT Configuration Tool to connect to the LAN2 IP addresses (IP Address “C” and “D” in the preceding table). These addresses are used for direct Gateway-to-Gateway communication only.

Determining the Role and State of the connected XRT

When connecting to a XRT with the XRT Configuration Tool, it is very important to know the Gateway’s role (Primary/Secondary) and current control state (Active/Inactive). The XRT Configuration Tool Status Bar shows the Gateway’s role and site control state (active or inactive) after connecting to the device. The Status bar of the connected XRT Gateway will show one of the following:

- Stand-alone Gateway (The Stand-alone is always in control since it is the only XRT)
- Primary Gateway Active (configured for the Primary role, and currently in control)
- Secondary Gateway Inactive (configured for the Secondary role, and currently not in control)
- Secondary Gateway Active (configured for the Secondary role, and currently in control)
- Primary Gateway Inactive (configured for the Primary role, but currently not in control)

Important! If any changes need to be made to the XRT configuration, such changes should be configured into the active XRT. The active XRT will automatically share the changes with the inactive XRT.

Maintaining the Primary and Secondary Gateways at same Firmware level

It is important to maintain the Primary and Secondary Gateways at the same XRT firmware version.

- Make sure the Primary and Secondary Gateways are at same firmware level prior to initial deployment of the Redundant Gateways.
- For field upgrades, both Gateways should be upgraded when upgrading to a new XRT firmware build. (Note: This requires two separate files because each XRT must always have its own firmware file. The file name should be the same except for the serial number, which is the last part of the file name.) For more information, please consult the release upgrade instructions.

Configuring the Primary and Secondary Gateway

It is recommended to perform initial configuration at the shop, prior to installing the XRT(s) at the deployed location. If adding a Redundant XRT to a previous, stand-alone unit, only the Secondary Gateway needs to be configured at the shop, since the Primary went through this process prior to its original deployment. Some configuration is still required for the Primary Gateway, but this can be accomplished at the deployed location if necessary.

As a general rule of thumb, do not connect the XRTs directly (LAN 2 on Primary to LAN 2 on Secondary) until both Gateways have been initially configured and are ready for redundant operation. This will help prevent the Secondary Gateway from attempting to assume control before you are ready. The Secondary Gateway will not attempt to take over site control until it has synched at least one time with the Primary via the LAN2 connection.

The following outline shows the steps that must be performed before the Redundant Gateway feature will be operative. Do not connect the LAN 2 ports prior to the point mentioned in the outline. This outline assumes that at least one Gateway has been previously configured for site control. If this is not the case, follow the installation and configuration guidelines outlined in the XRT Gateway User Guide.

1) Configuring the Secondary Gateway

   a) If the Secondary Gateway is “fresh out of the box”, the first step is to establish communication with the Gateway. Because the Gateway comes with a default IP address, you may have to edit the IP address on your PC for the first connection. See the XRT Gateway User Guide for details. When initially configuring the IP address that will be used for this Gateway, enter the address into the Primary IP Address field (for LAN 1) and leave the Gateway role as “stand-alone”. In a later step, the Gateway role will be changed to “Secondary”, and its IP address will be configured into the Secondary IP address field (for LAN 1).

   b) The Network Time Protocol (NTP) Configuration for the two Gateways that will serve as Primary and Secondary for the same deployment must be configured the same. If the Primary will serve as the network’s NTP Server, then the Secondary must also be configured as network’s NTP Server. If the Primary is configured to point to another IP address as NTP Server, then the Secondary must also point to the same NTP Server.

   c) Manually set the clock on the XRT that will serve as the Secondary Gateway in order to bring it as close as possible to the NTP Server time. This important step helps this XRT to synch its time with the NTP server more quickly (once a connection is established to the NTP Server). Set the date and time from the Date & Time Configuration screen (Settings→Date and Time).

   d) Configure the Network Settings of the Secondary Gateway for field operation (Network→Settings).

      i) Set the Role as “Secondary”.

      ii) Configure Network IP Addresses, Network Properties, and IP Addresses to be used at the site. It is important to note that these fields must be configured with identical information in both the Primary and Secondary Gateway, and that the configured values do not change – even when the Secondary Gateway automatically assumes the Primary Gateway’s IP address and becomes the “active” site Gateway.

   e) After saving the Network Settings the Secondary Gateway will reboot and come back with its new IP address. It will probably be necessary to make one or more changes (such as editing the PC’s IP address, re-defining the IP address used to connect, taking the Gateway to where it will be deployed, etc.) prior to communicating with this XRT again.

2) Configuring the Primary Gateway. (Instructions assume that this is a previously operating Gateway that has already been configured with most settings.)

   a) Connect to the XRT that will be used as Primary Gateway.

   b) Since it is important to always have a current backup file for each Primary XRT, use the XRT Configuration Tool Backup & Restore Utility to make a backup file of this gateway (Settings→Backup & Restore Utility). Performing the backup prior to configuring the Network Settings (as described in the next step) is acceptable because the Network Settings information is intentionally omitted from the backup file.

   c) Open the Network Settings screen (Network→Settings).

      i) Configure the Role as “Primary”

      ii) Configure Network IP Addresses, Network Properties, and IP Addresses to be used at the site. It is important to note that these fields must be configured with identical information in both the Primary

and Secondary Gateway, and that the configured values do not change – even when the Secondary Gateway automatically assumes the Primary Gateway's IP address and becomes the "active" Gateway.

d) After saving the Network Settings the Primary Gateway will reboot. It will be necessary to re-connect, if desired.

Making the physical connections (assumes that configuration is complete)

1. Bring both Gateways to the deployment location (if not done already)

2. For an existing installation, the Primary Gateway will already be connected to the Ethernet switch.

3. Connect the Secondary Gateway to the Ethernet switch (connecting via the LAN1 port on the Secondary Gateway).

4. Plug in the direct connection between the two ports labeled "LAN2" on the Primary and Secondary Gateways.

5. Provide power to the Secondary Gateway. After the Secondary Gateway finishes booting up, it will communicate with the Primary Gateway. The Primary and Secondary will then start the process of synchronizing important settings. This process can take several minutes, depending on how much information needs to be shared. See the next section for more information.

Important: Prior to leaving the installation location, it is strongly recommended that the technician perform a test to verify the redundant operation. The specific instructions for this test are provided in a later section.

Primary and Backup Gateways synchronize certain information

After establishing the direct connection between the Primary and Secondary Gateway, the two XRTs will automatically synchronize the following important information:

1. If the user database is not already identical in both Gateways, then the user database from the active XRT will replace the user database in the inactive XRT. This process can take up to five minutes, depending on the size of the user database in the active Gateway. If the user database in both Gateways is already identical, this step is omitted.

2. Settings contained on the active Gateway's Configuration Screen will replace the Configuration settings for the inactive Gateway.

3. Settings contained on the active Gateway's Multisite Configuration Screen will replace the Multisite settings for the inactive Gateway.

4. Settings contained on the active Gateway's XRT User Configuration Screen (Settings→XRT User Configuration) will replace the XRT User Configuration settings for the inactive Gateway.

5. The list of units and groups currently registered into the network (at other sites), as well as their present site location.

6. SMTP Setup and Alert Notifications that have been configured into the active Gateway will replace the SMTP Setup and Alert Notifications settings for the inactive Gateway.

7. Certain network messages that have been sent to other sites, but have not yet been acknowledged by the destination site.

In order to determine when the synch process is complete, connect to the Primary Gateway with the XRT Configuration Tool and view the Alerts/Alarms Management Screen (Alerts/Alarms→Alerts/Alarms Management). The Primary Gateway will show an Alert that says, “Primary Gateway missing connected Secondary Gateway”. Press the “Clear” button to clear this Alert, and then wait for five seconds and press the “Refresh” button. If the Alert does not reappear, then the synch process is complete, and the Secondary Gateway is ready to assume site control when needed.

Continued Sharing of Information

Following their initial synchronization, and for as long as the active and inactive Gateways have a LAN2 connection, the active Gateway continues to automatically update the inactive Gateway when there are changes to any of the information that was shared during the initial synchronization process described in the previous section.

The active XRT also informs the inactive XRT whenever a user initiates a voluntary reset of the active Gateway. The term “voluntary reset” includes the following:

1. Reboot command issued via the XRT Configuration Tool.

2. Reboot after a “critical” setting is updated via the XRT Configuration Tool and saved to XRT.
    a. Any setting in “Critical Settings” portion of Configuration screen. (Settings→Configuration)
    b. Any setting on the Network Settings screen. (Network→Settings)
    c. Any setting on Multisite Configuration screen. (Settings→Multisite)

3. Reboot after a configuration file is uploaded via the Restore tab on the XRT Configuration Tool “Back and Restore” utility.

4. Reboot after a Firmware Upgrade command issued via the XRT Configuration Tool.

Following a voluntary reset, an Inactive Secondary Gateway allows the Primary Gateway a period of time to reboot and resume control. If the Primary XRT does not come back on line within the expected period of time, the Secondary XRT will attempt to take over control.

Information not shared

It is also important to understand that there is some information that is not shared between the active and inactive Gateways. This includes the following:

1. Information on current calls. These do not carry over when there is a switchover in site control from the active to the inactive Gateway.

2. The list of active network connections with sites listed on the Multisite Table. (When a Gateway takes over site control, it will attempt to set-up new connections with all sites on its Multisite Table.)

3. Event Log Data. This is only saved to the currently active Gateway.

4. Alerts that are currently active on the other XRT device in the redundant pair.

5. Currently connected XRT Client(s), as well as information on the sockets that were established when the Client(s) connected.

6. Talk Paths registered by XRT Clients.

7. Pool IDs registered on behalf of XRT Clients.

8. Information pertaining to raw data packets originated by a XRT Client.

Automatic Switch of Site Control

The active and inactive Gateways exchange heartbeat messages over their LAN2 direct connection. Automatic switchover is supported for any scenario that results in the loss of heartbeat messages between an active Primary and inactive Secondary Gateway. Examples include (1) power failure on Primary XRT (2) Hardware failure affecting IP ports on the Primary XRT, (3) Connect Plus software program stops running on Primary XRT. Switchover occurs following expiration of an internal timer in the Secondary XRT.

Note: There are some scenarios where the Secondary XRT may attempt to take over control, but not be able to so. An example of such a case is when the LAN2 connection between the two Gateways fails, but the Primary Gateway still has a good LAN1 connection to the Ethernet switch (and to the XRT Clients and other sites). In this event, the Primary Gateway will not relinquish its Primary LAN1 IP address. If the Secondary XRT attempts to take over control due to a Failover Trigger, but is not able to take over the Primary LAN1 IP address, it will create an Event Log entry and periodically retry.

Figure 2-1 illustrates Redundant Gateway connections after control switches from the Primary to Secondary Gateway.

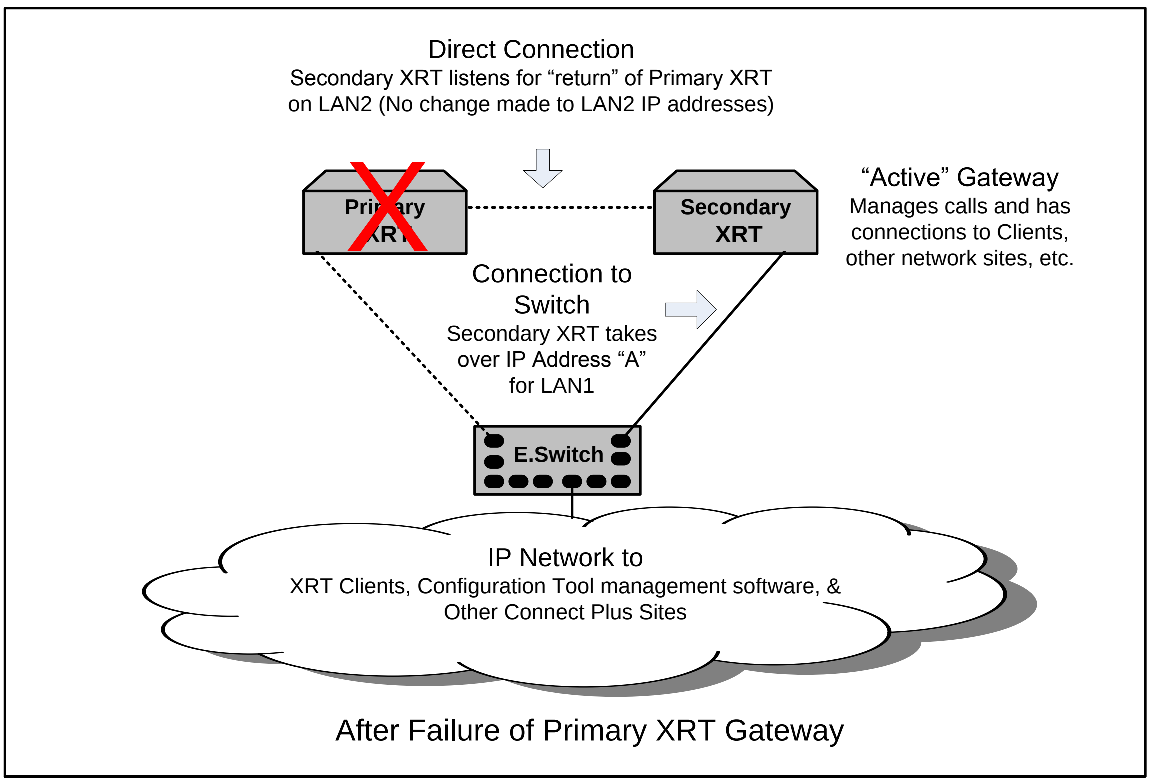


Figure 4-14 Redundant Gateway Configuration with Secondary XRT Active

Swapping LAN1 IP Addresses

Whenever a Gateway switchover occurs, the (newly) active XRT Gateway will take-over the IP address that has been configured with the XRT Configuration Tool as the "Primary IP Address" for LAN1. (IP Address "A" in the preceding table.) In other words, this is the IP address for the "active" Gateway, regardless of whether it is the Primary or Secondary.

If a XRT attempts to use the IP address that has been configured with the XRT Configuration Tool as the "Primary IP Address" for LAN1, but finds out the address is already in use, it will assume the "inactive" state, and will instead use the IP address that has been configured with the XRT Configuration Tool as the "Secondary IP

Address" for LAN1. An example of such a case is when the Secondary Gateway has taken over site control, and then the Primary Gateway subsequently comes back on line. The Primary Gateway shall make one attempt to use the Primary LAN1 IP address. Upon finding that the "Primary" address is already in use, the Gateway will use (or attempt to use) the "Secondary" address for as long as it remains in the "inactive" state, even though its configured role remains that of "Primary" Gateway.

In order to swap IP addresses as described in this section, the LAN Ethernet switch must be able to accept a gratuitous ARP response, and change a previously registered IP address. If there is any question about whether the LAN Ethernet switch will accept gratuitous ARP responses, check the switch configuration or consult the company IT specialist. A subsequent section describes a test that, if passed successfully, confirms that the LAN Ethernet switch accepts gratuitous ARP responses.

Manual Switchover initiated via the XRT Configuration Tool

In addition to the failure scenarios that cause automatic switchover from the Primary to Secondary Gateways, switchover can also be initiated via a Configuration Tool Menu command. The switchover command should always be given to the active Gateway. It is useful for the following:

1. Technician wishes to switch control from Primary to Secondary Gateway in order to perform maintenance on Primary Gateway.

2. Technician wishes to switchover site control from an active Secondary Gateway back to the Primary Gateway (usually after completing repair or replacement of Primary Gateway). Because there is no automatic switchover from Secondary to Primary, the Menu command is the only way this can be accomplished. If it is necessary to replace the former Primary Gateway with another XRT, use the XRT Configuration Tool to perform some basic configuration on the (new) Primary Gateway prior to switching site control back to the Primary. Perform the following configuration at the shop prior to bringing the (new) Primary Gateway to the installation location:

    a. If the (new) Primary Gateway is "fresh out of the box", the first step is to establish communication with the XRT. Because the Gateway comes with a default IP address, you may have to edit the IP address on your PC for the first connection. See the XRT Gateway User Guide for details. When initially configuring the IP address that will be used for this Gateway, enter the address into the Primary IP Address field (for LAN 1) and leave the Gateway role as "stand-alone". In a later step, the Gateway role will be changed to "Primary" and its IP address will be configured into the Primary IP address field (for LAN 1).

    b. The Network Time Protocol (NTP) Configuration for the two Gateways that will serve as Primary and Secondary for the same site must be configured the same.

    c. Manually set the clock on the (new) Primary XRT in order to bring it as close as possible to the NTP Server time. Set the date and time from the Date Time Configuration screen (Settings→Date and Time).

    d. Configure the Network Settings Screen of the (new) Primary Gateway for field operation (Network→Settings).

    e. Set the Gateway Role as "Primary".

    f. Configure Network IP Addresses, Network Properties, and Redundant Gateway Feature IP Addresses to be used at the installation location. It is important to note that these fields must be configured with identical information in both the Primary and Secondary Gateway.

    g. After completing the configuration above at the shop, transport the (new) Primary XRT to the installation location, connect its LAN1 port to the LAN Ethernet Switch, connect its LAN2 port directly to the LAN2 port on the active Secondary XRT (using the Ethernet Crossover Cable), and apply power to the (new) Primary XRT. The (new) Primary XRT will discover that the Primary Gateway IP Address is already in use. It will go to the "inactive" state, and it will use the Secondary Gateway LAN1 IP address. When the

two Gateways establish communication via their LAN2 connection, the Gateways will synchronize important settings as described previously. In this scenario, the settings in the active Secondary XRT take precedence and will replace the settings in the inactive Primary XRT.

h. When the two Gateways have finished the synch process, use the XRT Configuration Tool to connect to the active Secondary XRT (connecting to the Primary Gateway LAN1 IP Address), and give the "Switch to Primary Gateway" command (Site Control→Switch to Primary Gateway).

Note: If the technician attempts to manually switch control by using either the "Switch to Primary Gateway" or "Switch to Secondary Gateway" command before the two devices have completed the synch process, the XRT Configuration Tool returns a message, which advises that the switch command was rejected. Should this occur, wait a few minutes and then attempt to give the switch command again.

Operation during switchover

The switchover process causes an interruption to communications. Calls in progress and queued calls are not maintained through a Gateway switchover. Operation will normalize when switchover is complete, and when the XRT Clients have re-established communications, re-authenticated, and re-registered Talk Paths with the new, active XRT.

Determining XRT Status

The XRT and the XRT Configuration Tool provide several indications to determine a Gateway's current status and whether a switchover has occurred:

Configuration Tool Status Bar: As discussed previously, when the XRT Configuration Tool connects to a XRT, the Status Bar tells the "role" of the connected XRT. If the "role" is "Primary" or "Secondary", the dashboard also tells the current state, "active" or "inactive".

Event Log Entries: When the Secondary Gateway has established connectivity to the Primary Gateway, and then has subsequently lost the heartbeat messages for a period of time, the Secondary Gateway writes a "Gateway Absent" message to the Event Log.

When either the Primary or Secondary Gateway switches states (inactive to active, or vice versa), it places a "Gateway Switch State" entry in the Event Log. The message shows the gateway's state, active or inactive.

The inactive Gateway will create a "Gateway Switch State Failure" Event Log entry if it attempts to switch to the active state, but is not able to take over the Primary LAN1 IP address.

Gateway Alerts: Gateway Alerts can be viewed on the XRT Configuration Tool's Alerts Management Screen. Gateway Alerts do not clear automatically. They must be cleared by the System Administrator or Technician after determining that the condition which triggered the Alert no longer exists. If the underlying trigger still exists, the Gateway Alert will return.

Alerts can be viewed and managed on the active Gateway only. They cannot be viewed or managed on the inactive Gateway. When a XRT changes to the inactive state, it clears any Alerts that may have been active on that XRT.

There are two alerts associated with Redundant XRT operation:

Primary Gateway missing connected Secondary Gateway: This alert indicates that the Primary Gateway hasn't yet communicated with the Secondary Gateway, or that communication has been established, but the process of synching with the Secondary Gateway is not yet complete. It can also indicate that the Primary Gateway has lost communication with the Secondary Gateway. If the System Administrator or Technician clears the alert, and it stays clear, this indicates that communication has been established, the synch process is finished, and the Secondary Gateway is ready to take over site operations, if necessary.

Secondary Gateway Active: This alert is generated when the Secondary Gateway takes over site operations.

Testing the switchover capability

After configuring and connecting the redundant Gateways, the technician should test switchover functionality, using the same LAN Ethernet switch that is used (or will be used) at the installation location. The steps for the test are listed below. The test will cause an interruption to XRT Client service at two points (switchover from Primary to Secondary, and switchback from Secondary to Primary). For this reason, it should be performed at a time when activity is low.

1. Complete all configuration and connections as described previously.
2. Use the XRT Configuration Tool to connect to the IP address that has been configured into the Gateways as the Primary IP address for LAN1.
3. After making the connection, look at the Status Bar. It should display, “Primary Gateway Active”.
4. From the Main Menu, select Site Control→Switch to Secondary Gateway
5. Acknowledge the warning message. This will reset the XRT and disconnect you from the device.
6. The switchover takes place, causing a temporary interruption to service.
7. Use the XRT Configuration Tool to connect to the IP address that has been configured into the Gateways as the Primary IP address for LAN1.
8. After making the connection, look at the Status Bar. At the bottom of this box it should say, “Secondary Gateway Active”. Assuming that you are connected via the site’s LAN Ethernet Switch, this confirms that the switch accepted the secondary’s gratuitous ARP response.
9. From the main menu, select Alerts/Alarms→Alert Management. This opens the Alerts/Alarms Management screen. There should be an active Alert for “Secondary Gateway Active”.
10. From the Main Menu, select Site Control→Switch to Primary Gateway.
11. Acknowledge the warning message. This will reset the XRT and disconnect you from the site.
12. The switchover takes place, causing a temporary interruption to service.
13. Use the XRT Configuration Tool to connect to the IP address that has been configured into the Gateways as the Primary IP address for LAN1.
14. After making the connection, look at the XRT Configuration Tool Status Bar. It should display, “Primary Gateway Active”. Assuming that you are connected via the site’s LAN Ethernet Switch, this confirms that the switch accepted the primary’s gratuitous ARP response. Site Control has now been returned to the Primary.

4.7 Connect Plus Data Sub-System Design Considerations

As discussed in previous sections, the Text Messaging application server is utilized with Connect Plus to allow Text Messaging client applications to exchange messages with the MOTOTRBO subscribers. Unlike the other MOTOTRBO digital modes the server connects to the XRC controller via a UDP/IPv4 connection. The same is true for the Location Tracking server. These server applications run on PC machines that require IPv4 address assignments and should be taken into considerations when designing the supporting IP network.

Moreover, all the IP-capable data devices can be dispersed across multiple networks, some of which are directly connected to the public Internet and others isolated and protected by firewalls. Connect Plus has been architected to operate over such heterogeneous networks.

4.7.1 Connect Plus Example System IP Plan

Figure 4-15 shows a hybrid network configuration with 6 sites where sites 1-4, and 5-6 respectively, are placed on private networks, but interconnected through the public Internet and protected with firewalls on each side. The diagram is provided as an example of how port forwarding can be utilized to send messages to multiple site controllers via a single IP address (the network firewall). It should be noted that another approach (which is highly recommended, but not pictured here) would be to place all 6 sites in the same Virtual Private Network (VPN) or closed private network (see "Connect Plus Simplified Example IP Plan"). The VPN approach allows each site controller to be addressed via a unique IP address, thereby eliminating the need for port forwarding.

Note that only the controllers (XRC) are shown for each site and the repeaters are omitted for better clarity. For this example, the repeaters should have IP addresses in the following subnets:

- 10.0.0.X for Sites 1-4
- 192.168.0.X for Sites 5-6

These IPv4 addresses can either be statically provisioned or acquired through DHCP. The important part is that the controllers are configured with static addresses.

Each of the border routers is capable of providing Network Address Translation with port forwarding, such that the IP traffic coming from the public side can reach the target controller via the public address and a predefined port number. Here the firewalls are shown as a logical components rather than physical boxes. It is quite common that the routers themselves function as firewalls.

The public IPv4 addresses are just examples of what an ISP will provide when a customer signs up for broadband service. Connect Plus does not currently support addressing sites through DNS domain names, so it is necessary to request public IPv4 addresses from the service provider.
Finally, the TMS Server and the LRRP (Location) Server are assigned private IPv4 addresses from their respective private address pools (refer to the diagram).

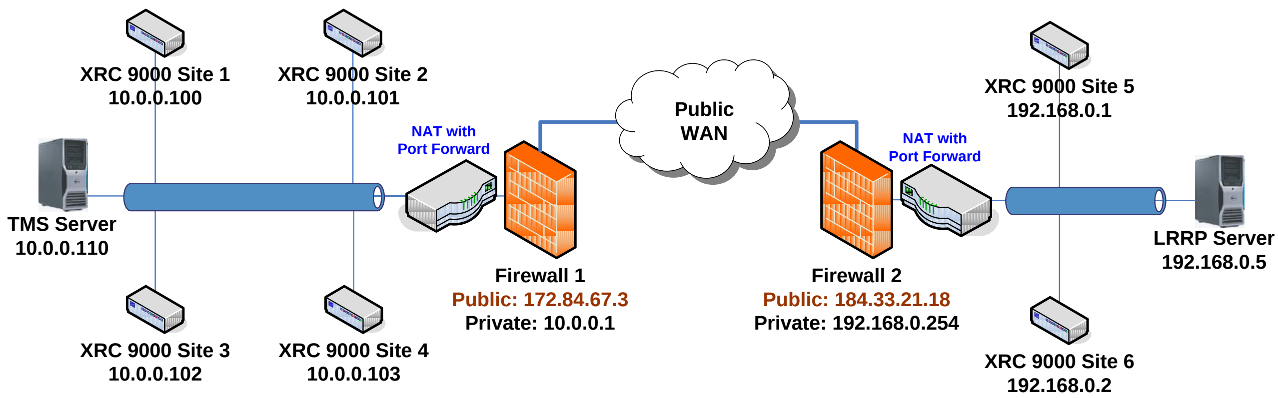


Figure 4-15 Example System IP Plan

The following table is provided for better understanding of IP data flows between the Connect Plus sites. For example, if the controller at Site 4 wants to send packets **to** the controller at Site 5, it needs to target it through the public IPv4 address 184.33.21.18.

SENDING TO	SENDING FROM XRC @					
	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6
Site 1	*	10.0.0.100	10.0.0.100	10.0.0.100	172.84.67.3	172.84.67.3
Site 2	10.0.0.101	*	10.0.0.101	10.0.0.101	172.84.67.3	172.84.67.3
Site 3	10.0.0.102	10.0.0.102	*	10.0.0.102	172.84.67.3	172.84.67.3
Site 4	10.0.0.103	10.0.0.103	10.0.0.103	*	172.84.67.3	172.84.67.3
Site 5	184.33.21.18	184.33.21.18	184.33.21.18	184.33.21.18	*	192.168.0.1
Site 6	184.33.21.18	184.33.21.18	184.33.21.18	184.33.21.18	192.168.0.2	*

Table 4-8 IP Address Matrix for the Example System

4.7.2 Port Assignments and Forwarding

Since the single public IPv4 address is in a way “shared” among the devices with private addresses, there has to be a mechanism to distinguish the private destination of the IP datagrams when they are received at the border router (from the public network).

A standard method to achieve this is by using a socket, which by definition is a pair of an IP address and port number. Depending on the IP payload, ports can be either TCP or UDP types.
Connect Plus utilizes sockets to allow the border router to direct the public IP traffic to the correct target device, such as a controller or an application server.

For further information on how to allocate and configure ports for the Connect Plus system the reader can reference [4]. The port assignments provisioned into the XRC controllers need to be noted by the system administrator and used to configure the NAT router. Most NAT routers allow Port Forwarding configurations for both, single (TCP or UDP) port and a range of port numbers.

The table below shows an example of Port Forwarding configuration for the system depicted in Figure 4-15. Here the assumption is that the TCP and UDP port assignments are the same for the external and internal port numbers. In other words, for **XRC Site 1** TCP packets received on socket 172.84.67.3**:**45001 will be forwarded to 10.0.0.100**:**45001.

Site	Private IP	NAT Public IP	TCP Control Port	UDP Voice Port Start	UDP Voice Port End
XRC Site 1	10.0.0.100	172.84.67.3	45001	46000	46031
XRC Site 2	10.0.0.101	172.84.67.3	45002	46032	46063
XRC Site 3	10.0.0.102	172.84.67.3	45003	46064	46095
XRC Site 4	10.0.0.103	172.84.67.3	45004	46096	46127
XRC Site 5	192.168.0.1	184.33.21.18	45005	46128	46159
XRC Site 6	192.168.0.2	184.33.21.18	45006	46160	46191

Table 4-9 Port Forwarding Example

4.7.3 Connect Plus Simplified Example IP Plan

Figure 4-16 presents multisite configuration with 3 Connect Plus sites with 3 repeaters per site, providing 5 trunked channels. The network topology is private LAN/WAN, which does not require any special port forwarding or network address translation. Each XRC controller can directly communicate with the other site controllers via their configured IP addresses. The reader can refer to Appendix B for more information and another example of private IP network topology.

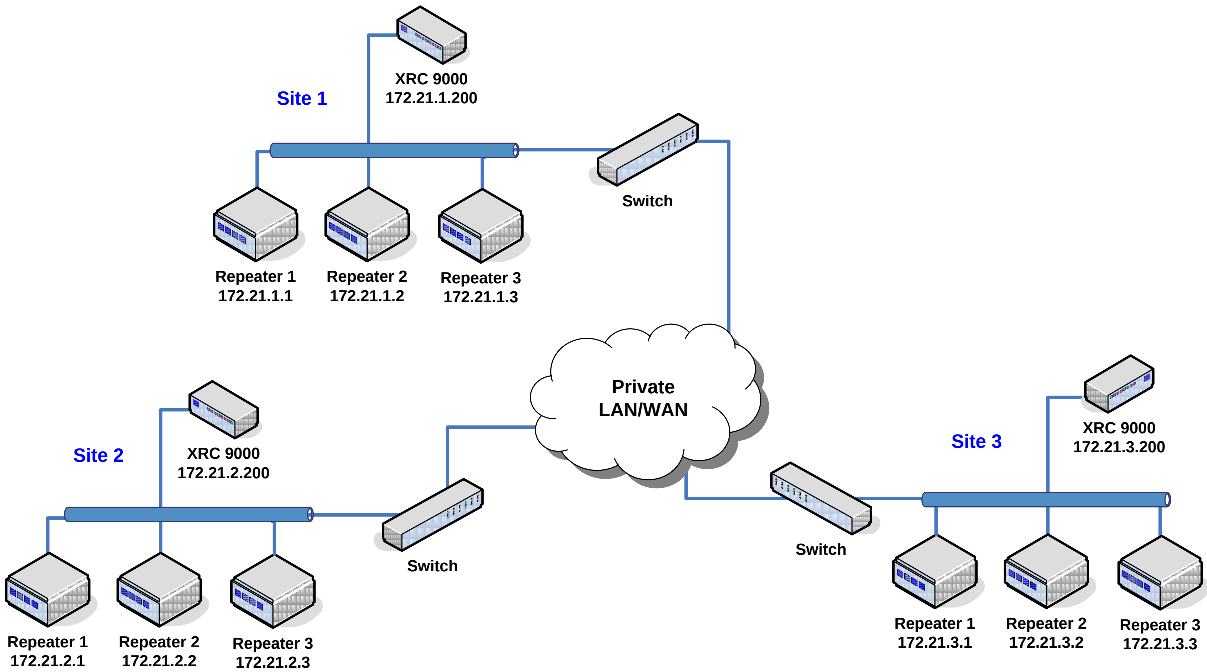


Figure 4-16 Simplified Example IP Plan

4.8 RF Resource Allocation

The following sections describe how the XRC allocates RF resources (trunk-to timeslots) at its local site. Understanding the points discussed in these sections will assist the radio system administrator in managing the site's RF resources.

4.8.1 Configurable Parameters for number of "Allowed Sessions"

For the XRC, all non-emergency call sessions fall into one of the two following major categories:

- **Outbound Data Sessions**
  The call types in this category are non-emergency location request/reports, text message delivery from the XRC to a destination SU (regardless of whether the text message was initiated by another SU or by a 3rd party text message application), Packet Data Call and Generic Data Call originated by an XRT Client and destined for a Connect Plus SU, and Connect Plus Over-the-air (OTA) unconfirmed file transfer. Each Fast GPS Report Channel also counts as one Outbound Data Session, even though all report transmissions are inbound to the channel.

- **Voice & Inbound Data Sessions**
  The call types in this category are Group Call, Multigroup Call, Site All Call (voice), Network Wide All Call (which utilizes the Site All Call Voice ID), Private Call, and inbound data. At the current time there is one call session classified as inbound data – text messages from the SU to the XRC.

The XRC has two programmable parameters used to determine how many calls for each category the controller will allow to be assigned at any one time.

Number of Outbound Data Sessions Allowed: This setting determines how many simultaneous sessions the XRC will allow for call types in this category. The XRC will continue to allocate timeslots (if available) for calls in this category until the site reaches the configured value. If no timeslots are available, or if the site reaches the configured value for “Number of Outbound Data Sessions Allowed”, subsequent calls in this category are not placed in the Busy Queue. They are queued in the Data Scheduler until the XRC allocates a timeslot for outbound data sessions. The Data Scheduler is a software module in the XRC that is responsible for scheduling and requesting RF resources for most outbound data sessions. The Fast GPS Report Channel is a special case. Each Fast GPS Report Channel is considered as one Outbound Data Session, even though all report transmissions are inbound to the channel. The controller will not allocate a timeslot for outbound data sessions as long as the number of simultaneous calls for call types in this category remains at the configured value. Because sessions in this category are not placed in the Busy Queue, sites with a lot of outbound data activity (such as GPS updates) may wish to reserve one or more timeslots specifically for outbound data. This will allow outbound data sessions to continue; even when all voice/inbound data slots are busy. For more information on how to achieve this objective, please see the section titled “Timeslot Allocation Using Call Sessions Configuration Parameters”. **Note**: For sites that utilize “Fast GPS Report Channels”, the “Number of Outbound Data Sessions Allowed” must be at least one greater than “Number of Fast GPS Report Channels Allowed”.

Number of Voice/Inbound Data Sessions Allowed: This setting determines how many simultaneous sessions the XRC will allow for call types in this category. The XRC will continue to allocate timeslots (if available) for calls in this category until the site reaches the configured value. If no timeslots are available, or if the site reaches the configured value for “Number of Voice/Inbound Data Sessions Allowed”, subsequent calls in this category are placed into the Busy Queue. When there are calls in the Busy Queue, and a timeslot becomes available, the XRC checks to see how many calls in this category are currently active on the site. If the number is below the configured value, the call at the top of the top of the Busy Queue is assigned to the available timeslot. If the “Number of Voice/Inbound Data Sessions Allowed” is equal to or greater than the configured value, the XRC operates as follows:

- If “Number of Outbound Data Sessions” is less than the configured value, the timeslot will be made available to the Data Scheduler for a call type in that category.

- If both the “Number of Voice/Inbound Data Sessions Allowed” and “Number of Outbound Data Sessions Allowed” are equal to or greater than the configured values, then the timeslot goes unused until at least one of the two counters drops below the configured value. In the meantime, the timeslot is available for Emergency Voice Calls and Emergency Location Updates.

It is important to note that Emergency Voice Calls and/or Emergency Location Updates are not subject to the rules discussed above. Their rules are as follows:

1. If *any* timeslot is idle, it will be used for Emergency Voice Call or Emergency Location update, regardless of the two counters discussed above. **Note**: Fast GPS Report Channels are not considered to be idle. They are used for periodic location reports only. They are not used for Emergency Voice Call or Emergency Location Update.

2. If no timeslot is available, the Emergency Voice Call or Emergency Location Update will be assigned to the Busy Queue and will receive priority for the next available timeslot per the rules discussed in the “Busy Queue” Section.

4.8.2 Timeslot Allocation Using Call Sessions Configuration Parameters

By understanding the operation of the two parameters discussed in the previous section, and by applying the formulas discussed below, the radio system administrator can achieve specific objectives for timeslot allocation. These objectives may vary according to priorities of the end user and the call types most commonly used. The next section provides some formulas, and the subsequent section provides some examples of how the formulas can be applied to achieve specific objectives.

4.8.2.1 Calculations to assure a minimum repeater bandwidth for specific call types

In this section, the term "bandwidth" refers to the number of repeater timeslots that the XRC makes available for calls in the "Outbound Data" and "Voice/Inbound Data" categories. The configuration strategies discussed in this section must be implemented on a per-site basis. Please note that the XRC does not provide the ability to reserve specific repeater timeslots for specific types of calls.

<u>To assure[47] a minimum bandwidth for Voice/Inbound Data</u>:

Total trunk-to timeslots	-	"Number of Outbound Data Sessions Allowed"	=	Minimum assured bandwidth for Voice/Inbound Data

<u>To assure[48] a minimum bandwidth for Outbound Data</u>:

Total trunk-to timeslots	-	"Number of Voice/Inbound Data Sessions Allowed"	=	Minimum assured bandwidth for Outbound Data

<u>To assure[49] a minimum bandwidth for Emergency Voice Call and/or Emergency Location Update</u>:

Total trunk-to timeslots	-	("Number of Outbound Data Sessions Allowed" **+** "Number of Voice/Inbound Data Sessions Allowed")	=	Minimum assured bandwidth for Emergency Voice Call and/or Emergency Location Update

4.8.2.2 Examples

Example A: There are 9 trunk-to timeslots available in the site. The radio system administrator wants the XRC to assign all calls "first come-first served" as long as there are timeslots available, regardless of whether the

[47] This assurance is only valid when there are no Emergency voice calls or Emergency Location Updates currently active or in the Busy Queue.
[48] This assurance is only valid when there are no Emergency voice calls or Emergency Location Updates currently active or in the Busy Queue.
[49] When there are no Emergency Voice or Emergency Location Update sessions on the system, these timeslots go unused. Also, note that the radio system administrator is not required to assure a minimum bandwidth for Emergency Voice and/or Emergency Location update if he/she is willing to make these calls spend a brief period of time in the Busy Queue when all timeslots are busy with non-emergency calls.

request comes from a radio user or from the Data Scheduler. He/she is not concerned with assuring a minimum bandwidth for either category. In this case, the radio system administrator sets the “Number of Outbound Data Sessions” to 9 or higher and “Number of Voice/Inbound Data Sessions” to 9 or higher.

Example B: There are 9 trunk-to timeslots available in the site. The radio system administrator wishes to reserve at least 3 trunk-to timeslots for outbound data sessions so that location updates can continue, even when there are voice/inbound data sessions in the Busy Queue. However, the radio system administrator does not wish the location updates to totally “crowd out” the voice calls. So, he/she sets the “Number of Outbound Data Sessions Allowed” to 6 and the “Number of Voice/Inbound Data Sessions” to 6. This means there will always be at least 3 timeslots available for outbound data sessions (as long as there are not any Emergency Voice Calls or Emergency Location Updates active or in the Busy Queue), but the number can go up to 6 depending on how many voice/inbound data calls are presently active. It also means there will always be at least 3 timeslots available for voice/inbound data sessions (as long as there are not any Emergency Voice Calls or Emergency Location Updates active or in the Busy Queue), but the number can go up to 6 depending on how many outbound data calls are presently active. In this example, it is important to understand the following:

1. When there are 6 voice/inbound data sessions active, the next request in this category is placed in the Busy Queue, even if there are slots not being presently used for outbound data.

2. When there are 6 outbound data sessions active, the XRC will not make any more timeslots available for outbound data, even if there are slots not being presently used for voice/inbound data. The outbound data sessions are not placed in the Busy Queue.

Example C: There are 9 trunk-to timeslots available in the site. The radio system administrator does not want the site to ever become so busy with non-emergency calls that the first Emergency Call has to wait in the Busy Queue. So, he/she sets “Number of Outbound Data Sessions Allowed” to 4 and the “Number of Voice/Inbound Data Sessions” to 4. Even when both categories are at the maximum (4 + 4), there is still one unused timeslot available for Emergency. It is important to note the following:

1. When there are 4 voice/inbound data sessions active, the next request in this category is placed in the Busy Queue, even if there are slots not being presently used for outbound data.

2. When there are 4 outbound data sessions active, the XRC will not make any more timeslots available for outbound data, even if there are slots not being presently used for voice/inbound data. The outbound data sessions are not placed in the Busy Queue.

3. When there are 4 calls in each category active, there is an available slot for Emergency. However, if no Emergency Calls or Emergency Location Updates are active, then this timeslot goes unused.

4. When there are 4 calls in each category active, and when there is also an active Emergency Call or Emergency Location Update, a second Emergency Call or Emergency Location Update will go into the Busy Queue.

For sites that use the Fast GPS feature, each currently active Fast GPS Report Channel timeslot counts as one outbound data session for the examples provided above. For more information on Fast GPS, see section “Connect Plus Fast GPS”.

4.9 MOTOTRBO CPS Programming Considerations

Connect Plus trunking logic resides in the Connect Plus Option Board, which communicates with main board of the MOTOTRBO radio to facilitate Connect Plus operation. Because the radio and the Option Board both play a part in this process, two different software programs play a role when configuring a Connect Plus Subscriber Unit. MOTOTRBO CPS is used to configure the radio's main board, while the Option Board is configured with Connect Plus CPS.

Although the majority of parameters associated with Connect Plus features are programmed with Connect Plus CPS, the importance of MOTOTRBO CPS programming cannot be over-stated. The radio must be programmed with MOTOTRBO CPS prior to using Connect Plus CPS to configure the trunking features. When configuring a Connect Plus radio with MOTOTRBO CPS, it is important to follow the guidelines provided in this document to ensure correct operation.

If the radio will contain only Connect Plus zones and channels, the MOTOTRBO CPS configuration is fairly straightforward because the programmer will not have to be concerned with screens that only affect non-Connect Plus modes. If the radio will be used for both Connect Plus and non-Connect Plus operation (such as MOTOTRBO analog & digital conventional modes or Capacity Plus), then CPS programming is more involved. The programmer will need to understand which settings affect only the non-Connect Plus modes, and which settings impact all radio modes, including Connect Plus.

The first step in configuring the SU is to use MOTOTRBO CPS to read the SU's codeplug. Then, from the MOTOTRBO CPS Main Menu select "View", and then select "Expert" from the drop-down View Menu. This will assure that the programmer sees all of the settings discussed in the following sections.

The following table provides a brief overview of the inter-relationship between MOTOTRBO CPS and Connect Plus. The headings in the left hand column are the major headings seen on the MOTOTRBO CPS Codeplug tree. If the table indicates that a particular screen is not used in Connect Plus, it can generally be by-passed if the radio is used for Connect Plus only. However, if the same radio is also used for non-Connect Plus modes, those screens should be configured according to the requirements of the non-Connect Plus application. This table provides an overview only. Before programming the radio, the programmer should also read the subsequent sections, which provide more detail on CPS dependencies and critical settings.

MOTOTRBO CPS Codeplug Tree	**Impact on Connect Plus Operation**
General Settings	Some settings are critical to Connect Plus operation
Accessories	When an accessory supported for Connect Plus operation is utilized, some of these settings impact Connect Plus, as well as other radio modes.
Buttons	Although Connect Plus buttons are programmed with Connect Plus CPS, some specific MOTOTRBO buttons affect Connect Plus operation if a feature is enabled while the radio is selected a non-Connect Plus zone and channel, and then the radio is changed to a Connect Plus zone and channel.
Text Messages	Not used for Connect Plus. Connect Plus Quick Text (pre-programmed) Messages are configured with Connect Plus CPS
Telemetry	Not currently supported for Connect Plus
Menu	Although Connect Plus menu operation is programmed with Connect Plus CPS, some specific MOTOTRBO menu options affect Connect Plus operation if a feature is enabled while the radio is selected a non-

	Connect Plus zone and channel, and then the radio is changed to a Connect Plus zone and channel.
Security	Connect Plus supports Enhanced Privacy. This screen is used to set the radio-wide Privacy Type (set to “None” or “Enhanced” for Connect Plus operation). If set to “Enhanced”, configure the Key ID, Key Alias, and Key Value columns on the table.
Network Settings	Some settings are critical to Connect Plus operation
Voice Announcement (some models)	Connect Plus supports some voice announcement capability in certain radio models. To enable this functionality, check the “Enable” box on the Voice Announcement screen, and perform the additional configuration described in the sections called, “Creating a Connect Plus Zone and Channel” and “Connect Plus Channel Settings”.
Signaling Systems	The majority of these settings are not used for Connect Plus. In some cases, Connect Plus CPS has similar parameters. The checkbox called “Emergency On/Off Switch” (provided for some radio models), does impact Connect Plus Emergency Call operation. If the radio user turns the power switch to the “off” position after his/her radio has requested an Emergency Call (and has been assigned to the traffic channel), the radio does not act on the power-down request until the Emergency Call has ended. Once the Emergency Call is over, the radio will power down. Several other facets of Connect Plus Emergency Operation are **not** impacted by this setting. If the radio user turns the power switch to the “off” position while the radio is in Connect Plus Emergency Pending state, or during Connect Plus Emergency Alert, the radio will power-down, regardless of whether the “Emergency On/Off Switch” box is checked or not.
Contacts	MOTOTRBO CPS contacts are not used for Connect Plus. Connect Plus Contacts are programmed with Connect Plus CPS.
RX Groups Lists	These lists are not used for Connect Plus
Channels	The way that Connect Plus zones and channels are organized with MOTOTRBO CPS is critical to Connect Plus operation. In regards to individual settings on the Channel screen, a few are critical to Connect Plus operation, but most are OK at default values. Many of the individual Channel settings will be overwritten with parameters configured with Connect Plus CPS.
Scan	These settings are not used for Connect Plus
Roam	These settings are not used for Connect Plus. Connect Plus Roam parameters are configured with Connect Plus CPS
Capacity Plus	These settings are not used for Connect Plus

When using MOTOTRBO CPS radio to configure a radio for Connect Plus, the main concerns of the radio programmer are to:

- Enable the Connect Plus purchasable feature.
- Set the Radio ID.

- Check settings that impact Connect Plus location updates & IP Data Operation. Many are OK at default values. Some may need to be adjusted slightly for optimal for Connect Plus operation.
- Create zones and channels for Connect Plus.

4.9.1 Enabling the Connect Plus Feature

Connect Plus operation is a purchasable feature for the MOTOTRBO radio. The SU can be programmed for Connect Plus prior to enabling the feature, but the Connect Plus Option Board will not enable its over-the-air signaling features until it verifies that the Connect Plus feature has been activated. Prior to feature activation, the Connect Plus SU will not search for service, attempt to register with any site, initiate calls, receive calls, etc. When an “unauthorized” radio is selected to a Connect Plus zone and channel, the LED blinks red and the radio sounds a tone. In addition, a display radio shows a message to inform the radio user that Connect Plus is not authorized.

The Connect Plus feature can be purchased through the Motorola Online (MOL) website. The process for purchasing, enabling, and viewing radio features is described in the following MOTOTRBO CPS Help screens:

- Purchasing Radio Features
- Activation
- View

MOTOTRBO CPS also provides a wizard to help walk the programmer through the process described in the Help screens listed above. The wizard is activated when choosing any item from the “Features” Menu with MOTOTRBO CPS.

After enabling the Connect Plus feature with MOTOTRBO CPS, it is necessary to recycle power on the radio. Upon power-up, the Option Board discovers that the Connect Plus feature is now enabled.

4.9.2 Setting the Connect Plus Radio ID

Each radio in the Connect Plus system must have a unique Radio ID, which is configured using MOTOTRBO CPS. The Radio ID field is located on the General Settings screen.

The radio uses the Radio ID as its individual ID for all digital modes. This includes not only Connect Plus, but also digital conventional and Capacity Plus.

MOTOTRBO CPS allows entries of 1 to 16776415 for the Radio ID. However, the top 64 numbers in this range (16776352 through 16776415) must not be used as the Radio ID for any Connect Plus radio. The Connect Plus system reserves these numbers for special purposes, so they must not be programmed into any radios. MOTOTRBO CPS will not block entry of these reserved values, so the programmer is responsible for entering a Radio ID that falls within the allowable Connect Plus range of 1-16776351. If the programmer enters any Radio ID higher than 16776351, the SU will not function correctly in the Connect Plus personality until the number is changed to a Radio ID that falls within the Connect Plus range.

Once a specific Radio ID is programmed into a Connect Plus SU, it cannot be used for any other Connect Plus SU network-wide. For this reason, it is very important to keep an accurate record of which radios have been

assigned which Radio IDs. The programmer should maintain an accurate list that shows both the MOTOTRBO Radio Serial Number (and the Physical Serial Number) and the Radio ID it has been assigned. This information must be entered into the controller database before the radio can be used on the Connect Plus system. The Serial Number and the Physical Serial Number are displayed on the MOTOTRBO CPS "Device Information" Screen.

4.9.3 Other General Settings Critical to Connect Plus Operation

After entering the Radio ID, the programmer should check the status of several other configurable parameters on the General Settings screen that impact Connect Plus operation:

- **GPS** (some models): Must be enabled for the SU to respond to Location Requests with current location coordinates obtained from the radio's GPS receiver. In some models, this setting is controlled only with MOTOTRBO CPS. In some models (and depending on how the radio is configured), the radio user can toggle the GPS receiver on or off.
- **Private Calls**: Must be enabled if this Connect Plus SU should be able initiate Private Calls.
- **TX Preamble Duration**: In Connect Plus, the TX Preamble precedes IP data transmissions only. It does not precede Connect Plus CSBKs. The TX Preamble should be set to **zero**.
- **Mic Selection Rule** (some models): This setting helps determine microphone audio routing in Connect Plus mode of operation.
- **Intelligent Audio Response** (some models): Determines whether the Intelligent Audio feature is enabled for all radio modes, including Connect Plus.
- **Voice Only**: If this setting is shown, the box must be <u>unchecked</u> (default setting) in order for the radio to transmit or receive any type of IP data. This includes text messages, location updates, and over-the-air file transfer.
- **Hot Mic Source**: In some radio models, this setting controls the Emergency hot mic audio routing in Connect Plus mode. In some radio models, the Emergency Hot Mic audio routing for Connect Plus mode is controlled by Connect Plus CPS configuration.
- **Disable ALL LEDs**: Determines whether LEDs are disabled for all radio modes, including Connect Plus.
- Under "Battery Saver", **Preamble** should be disabled (unchecked).
- Under "Alerts", **Disable All Tones** should not be checked, unless the programmer's desire is to disable all tones radio-wide, including Connect Plus zones and channels.
- **Channel Free Indication Tone**: Enables the Channel Free Indication tone in Connect Plus and other modes of operation.
- **Talk Permit Tone**: In some radio models, this setting controls the Talk Permit tone in Connect Plus mode. In some radio models, the Connect Plus Talk Permit tone is controlled by Connect Plus CPS configuration.
- **Persistent LRRP Requests**: If the radio is used for Connect Plus operation, do not check the "Save" box. This could interfere with Connect Plus operation.

- **Power Up Desired Channel**: If the radio is used primarily for Connect Plus operation, set this to "Last Selected Channel". If the radio is powered down in a Connect Plus zone, it will power up to the last selected Connect Plus zone and Call ID. This setting is not provided for all radio models.

4.9.3.1 MOTOTRBO CPS Button Settings and Connect Plus Operation

The General Rules for programmable button operations are as follows:

- When selected to a non-Connect Plus zone and channel, a programmable button operates as configured with MOTOTRBO CPS.

- When selected to a Connect Plus zone and channel, programmable buttons operate as configured with Connect Plus CPS.

4.9.3.2 MOTOTRBO CPS Menu Settings and Connect Plus Operation

The General Rules for menu operations are as follows:

- When selected to a non-Connect Plus zone and channel, the Menu operates as configured with MOTOTRBO CPS.

- When selected to a Connect Plus zone and channel, the Menu operates as configured with Connect Plus CPS.

4.9.4 Network Settings Critical to Connect Plus Operation

The following table lists the MOTOTRBO Network Settings that are critical to Connect Plus operation. Network Settings not listed on this table affect Non-Connect Plus channels only.

Setting	Connect Plus note
Radio IP	Radio IP. This is usually left at default setting of 192.168.10.1. Connect Plus will still operate correctly if value is changed.
CAI Network	Must be left at default value of 12
CAI Group Network	Must be left at default value of 225
Maximum Transmit PDU Size	Must be set large enough to accommodate the largest text message, data message, or LRRP Report transmitted by the radio while operating in a Connect Plus zone. If the radio is capable of sending a 280 character text message, set Max TX PDU to at least 750 bytes. Set to 1500 bytes to accommodate maximum possible location report size containing indoor location elements.

The Network Screen has several configurable port settings. As a rule, these settings affect non-Connect Plus zones and channels only, unless the programmer mistakenly selects a port number already used by the Connect Plus Option Board. To avoid conflicts with Connect Plus, the programmer must NOT use any of the following ports for these configurable settings; 4061, 4062, 4063, 4004.

Settings under the "Bluetooth" heading impact Connect Plus operation. However, Bluetooth Serial Data is not currently supported while selected to a Connect Plus zone and channel.

4.9.5 MOTOTRBO CPS Zone & Channel Configuration for Connect Plus

One of the most important aspects of MOTOTRBO CPS configuration for Connect Plus is setting up the zone(s) and channels that will be used by the Connect Plus Option Board. Most applications will require just a single Connect Plus zone with 16 channels enabled for "Option Board" and "Option Board trunking". This is because the Connect Plus SU can Roam to any site in the Connect Plus network while operating in just one Connect Plus zone. It's usually not necessary to have more than one Connect Plus zone unless additional zones are needed for a specific reason. The following list provides some examples, but there could be other reasons that also necessitate multiple Connect Plus zones.

- Radio user needs more than 16 Talk Groups. This would require more than one zone, since each Connect Plus zone supports a maximum of 16 assignable positions on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio).

- Connect Plus organizes its Contact list on a per-zone basis, with each Connect Plus zone providing a maximum of 100 contacts. If this number is not sufficient for the radio user; one or more additional zones would be required. In this case, it is possible that the zones might be programmed identically, except for the Contact list. Only the contact names (aliases) in the selected zone are visible to the user when using the subscriber menu and during active calls. The contacts in the **non-selected** zones are not accessible and the contact names are not displayed when these contacts key up during calls.

- Radio user with non-display portable or numeric display mobile wishes to initiate many Private Calls. Since these models don't have a menu, the only way to initiate a Private Call is by assigning a One Touch Call button or assigning a position on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio) for each destination Private Call ID. Since there are only 16 such assignable positions per zone, this may prompt a need for multiple Connect Plus zones.

The following rules <u>must</u> be followed when setting up Connect Plus zones and channels. It is the radio programmer's responsibility to know these rules and follow them because they are not enforced by the MOTOTRBO CPS software. These rules must be followed exactly in order for Connect Plus to operate properly. MOTOTRBO CPS supports "drag and drop" functionality for CPS zones in Zone table view. To see the Zone table view, select "Channels" in the codeplug tree view (in the left-hand pane). This causes MOTOTRBO CPS to display the Zone table in the right-hand pane (if supported by the CPS version). The most important column is the one labeled "Position". The numbers in this column show the order that the zones will be stored in the radio (after writing the codeplug) or the order that they are currently stored in the radio (after reading the codeplug). These enhancements can assist the MOTOTRBO CPS user in following the important Connect Plus rules for zone order and channel configuration. The zone order instructions written below (and in subsequent sections) are written so that they can be used with any version of MOTOTRBO CPS software and MOTOTRBO radio firmware:

- Each Connect Plus zone must have 16 identically configured channels that are enabled for both "Option Board" and "Option Board trunking". These are the only types of channels allowed in a Connect Plus zone.

- Non-Connect Plus channels (analog conventional, digital conventional, Capacity Plus, "talkaround" channels, etc) are NOT allowed in any Connect Plus zone.

- For the Display Portable and Display Mobile, Connect Plus supports a maximum of 16 Connect Plus zones per SU. Since each Connect Plus zone must be programmed with 16 identical channels, the maximum number of Connect Plus channels per SU for these models is 16 x 16 (for a total of 256

channels). For the Non-Display Portable and Numeric Display Mobile, the radio supports a maximum of two zones per SU. If both of these zones are used for Connect Plus, the maximum number of Connect Plus channels per SU for these models is 2 x 16 (for a total of 32 channels).

- Connect Plus zones must be at the top of the Channels list. They cannot be preceded by any non-Connect Plus zones. If there are multiple Connect Plus zones, they must be contiguous – starting with the first zone on the Channels list. For example, if the radio has 5 Connect Plus zones, they must be the first 5 zones in the Channel List. Any non-Connect Plus zone must come after these zones in the list. If the radio already has non-Connect Plus zones prior to adding Connect Plus zones, the non-Connect Plus zones will have to be moved so that they follow the Connect Plus zones. This procedure is described later in this document.

- The “Channel Pool” icon must come immediately after the first zone folder. Any other position for the Channel Pool icon would be unexpected, and would likely result in undesirable operation. If using a CPS version that supports the Zone table view, the “Position” Column must show the Channel Pool as being in Position #2. Because some CPS versions do not allow the CPS user to move the Channel Pool, it is very important to follow the steps outlined in the sections called, “Creating a Connect Plus Zone and Channel” and “Connect Plus Zone Placement within the Channel List”.

The steps for creating Connect Plus zones and channels are as follows. Each of these steps will be described in greater detail in subsequent paragraphs.

1. Programmer edits the first radio zone (and first digital channel in that zone) to create the first Connect Plus zone and the first Connect Plus Channel.

2. Programmer configures the Connect Plus channel settings.

3. Programmer copies & pastes the Connect Plus channel until the Connect Plus zone contains 16 identical channels.

4. If radio user needs multiple Connect Plus zones, the programmer copies and pastes the Connect Plus zone until the radio has the desired number of Connect Plus zones.

5. If the radio also has non-Connect Plus zones, then all Connect Plus zones must come before the non-Connect Plus zones. The final step is to move any non-Connect Plus zones below the Connect Plus zones so that the Connect Plus zones will be first in the list as required. Guidelines for this operation are provided in section called, “Connect Plus Zone Placement within the Channel List”.

4.9.5.1 Creating a Connect Plus Zone and Channel

The procedure for creating Connect Plus zones and channels is as follows:

1) In the MOTOTRBO CPS codeplug tree, locate the “Channels” folder, and then locate the first zone folder underneath the “Channels” folder. Step 2 describes how to edit this zone so that it will become the first Connect Plus zone. If the zone is already in use for a non-Connect Plus mode, you can copy the zone folder and paste the copy at the end of the Channels list by following these instructions:

   a) Right click on the zone folder
   b) Select “Copy” from the right click menu
   c) Right Click on the “Channels” folder
   d) Select “Paste” from the right click menu
   e) This will place a copy of the zone folder (and all of its channels) at the end of the Channels list
   f) Now, proceed to edit the first zone folder as described in Step 2.

2) Edit the first zone folder to convert it to the first Connect Plus zone as follows:

   a) Edit the folder name, if desired, by right clicking the zone folder and selecting “Rename” from the right click menu
   b) Delete all but one digital channel from this zone folder. To delete a channel, select the channel to be deleted, press the “Delete” key, and then click “Yes” to confirm the deletion. **Note**: if the folder does not have at least one digital channel already, add one by right-clicking on the zone folder and then selecting “Add Digital Channel”.
   c) Delete all analog channels from this zone folder. To delete a channel, select the channel to be deleted, press the “Delete” key, and then click “Yes” to confirm the deletion.
   d) After completing these steps, the zone folder should now contain just one digital channel. Click on the one digital channel, and edit the channel settings according to the instructions in the next section.

Enabling Voice Announcement for a Connect Plus Zone

For radio models that support the voice announcement feature, the radio can be configured to play a voice announcement upon selecting a Connect Plus zone. This feature requires configuration in both MOTOTRBO CPS and Connect Plus CPS.

1. In MOTOTRBO CPS:

   a. Enable Voice Announcement in the radio and load the voice announcement files.

   b. Select the “Channels” folder in the MOTOTRBO CPS tree view. In the right hand panel, the Channels window displays a table with Zone Names and a column labeled Voice Announcement File. Use this column to select the appropriate voice announcement file for each zone where the announcement is desired.

2. In Connect Plus CPS:

   a. On the General Zone Parameters screen for each zone where voice announcement is desired, enable the Zone Voice Announcement checkbox.

   b. When zone voice announcement is enabled as described above, the radio plays the configured zone voice announcement if the radio powers up in this zone, or if the radio user selects this zone following power-up. If the radio user desires to listen to the announcement “on demand” (without changing zones), this can be accomplished by configuring a “Channel Announcement” button with Connect Plus CPS. If the radio has been configured for both the zone announcement and channel announcement, then both announcements will play when the radio user presses the “Channel Announcement” button.

4.9.5.2 Connect Plus Channel Settings

View the settings on the Channel screen in the right-hand pane. Verify that all settings are being displayed by going to Main Menu, and then selecting “View”, followed by “Expert” from the drop-down view menu.

The Channel Screen has many settings, but the programmer only needs to be concerned with a few of them. That’s because most of these settings will be overwritten by parameters entered with Connect Plus Board CPS.

Settings that must be changed from default values

There are three settings that must be changed from the MOTOTRBO default settings for proper Connect Plus Operation.

Setting	Connect Plus note
Option Board Checkbox	Programmer must select (check) this box for Connect Plus operation
Option Board Trunking	Programmer must select (check) this box for Connect Plus operation
Admit Criteria	Change this setting to "Always" for Connect Plus operation. This assures the fastest possible system access times. For Connect Plus, setting the Admit Criteria to "Always" does not mean the radio will always operate impolitely. Connect Plus will still operate "politely" during Connect Plus calls.
In Call Criteria	Set this to "Always" for Connect Plus operation. For Connect Plus, setting the In Call Criteria to "Always" does not mean the radio will always operate impolitely. Connect Plus will still operate "politely" during Connect Plus calls.

All of the other settings should be OK at the default values. Because some of these settings are important to Connect Plus operation, the programmer should check the following parameters and verify that they are set as required by Connect Plus.

Settings that should be OK at default values, but should be verified by radio programmer

Setting	Connect Plus note
Phone System	Set this to "None" for Connect Plus operation
Privacy Checkbox	This box should always be disabled (unchecked) when programming the radio with MOTOTRBO CPS. This will not prevent the radio user from utilizing Enhanced Privacy when other Privacy settings are correctly programmed in MOTOTRBO CPS and Connect Plus CPS. For more information, see section "Connect Plus Voice and Data Privacy".
IP Site Connect Checkbox	This must be disabled (unchecked) for Connect Plus operation
Compressed UDP Data Header	This must be disabled for Connect Plus operation. Set "Compressed UDP Header" to "None". This will not prevent the Connect Plus radio from utilizing the MSI Compressed UDP Data Header when the XRC Controller expects it do so.
Channel Inhibit	This must be disabled (unchecked) for Connect Plus operation.
RX Only	This must be disabled (unchecked) for Connect Plus operation. If RX Only is desired, it must be programmed with Connect Plus CPS.
(RX) Reference Frequency	This must be selected to "Default"
(TX) Reference Frequency	This must be selected to "Default"
Contact Name	This must be selected to "None". This will be set via Connect Plus

	CPS.
VOX	This must be disabled (unchecked) for Connect Plus operation
TOT (Time Out Timer)	Connect Plus CPS has a settable TOT, which defaults to 60 seconds also. This setting must not be shorter than the Connect Plus CPS value.
TOT Rekey Delay	This must be set to 0 sec
Allow interruption	This must be disabled (unchecked) for Connect Plus operation
TX Interruptible Frequencies	This must be disabled (unchecked) for Connect Plus operation
Private Call Confirmed Checkbox	This must be disabled (unchecked) for Connect Plus operation. Connect Plus provides its own confirmation for Private Calls.
Data Call Confirmed Checkbox	This box must be enabled (checked) for Connect Plus operation. This will not prevent the Connect Plus radio from making unconfirmed data calls when the XRC Controller expects it do so.

Enabling Voice Announcement for a Connect Plus channel position

For radio models that support the voice announcement feature, the radio can be configured to play a voice announcement upon selecting a Connect Plus channel position. (Each Connect Plus channel position can be assigned to a specific Talk Group or Private Call contact). This feature requires configuration in both MOTOTRBO CPS and Connect Plus CPS.

1. In MOTOTRBO CPS:

    a. Enable Voice Announcement in the radio and load the voice announcement files.

    b. If the MOTOTRBO CPS configuration has been done correctly, for each zone utilized by Connect Plus, there will be a list of 16 digital channels. For each of these channels, there is a setting called Voice Announcement File. Configure the voice announcement file(s) that should play when the radio user selects the corresponding Connect Plus channel position.

2. In Connect Plus CPS:

    a. After completing the MOTOTRBO CPS configuration described above, use Connect Plus CPS to configure the Zone Channel Selections screen. Check the box labeled “Voice Announcement” for each channel position where voice announcement is desired.

    b. When zone voice announcement is enabled as described above, the radio plays the configured channel voice announcement if the radio powers up while selected to this channel, or if the radio user selects this channel following power-up. If the radio user desires to listen to the announcement “on demand” (without changing channels), this can be accomplished by configuring a “Channel Announcement” button with Connect Plus CPS. If the radio user presses the “Channel Announcement” button while selected to this channel, the radio will play the configured channel announcement.

Note: It is important to understand the relationship between the Connect Plus channel position and the order that the digital channels are listed with MOTOTRBO CPS. For example, if the user should hear a voice announcement when selecting the Connect Plus groups assigned to the first and third positions (but not the second position),

then configure voice files for the first and third MOTOTRBO CPS digital channels for that zone. However, on the second digital channel, the Voice Announcement File field can be set to “None”. In the Connect Plus CPS configuration for the corresponding Option Board zone, check the “Voice Announcement” checkbox for the first and third positions on the Zone Channel Selections screen. The checkbox for the second position should remain unchecked.

This concludes the set-up for this channel. It may seem unusual not to be concerned with settings such as “Color Code”, “Repeater Timeslot”, “RX Frequency”, and “TX Frequency”, but these settings are configured when building the Network Frequency File with Connect Plus CPS.

The next step will be to copy this channel and paste it 15 times to the Connect Plus zone, as described in the following section:

4.9.5.3 Verifying Number of Channels in Connect Plus Zone

Since Connect Plus requires 16 identically programmed channels in each Connect Plus zone, the easiest way to accomplish this is to create one Connect Plus channel, and then copy and paste it 15 times into the Connect Plus zone.

- In the MOTOTRBO CPS codeplug tree view, right click on the newly created channel, and select “Copy”.
- In the MOTOTRBO CPS codeplug tree view, right click on the Connect Plus folder and select “Paste”. This will place the copied channel into the folder. The folder should now contain two identically programmed channels.
- Repeat this process 14 more times
- At the completion of this process, count the channels in the folder to verify that there are exactly 16.

4.9.5.4 Creating Additional Connect Plus Zones (if necessary)

As stated previously, most radio users will only need one Connect Plus zone. However, if more than Connect Plus zone is required, it can be accomplished via a simple “copy” and “paste” approach as described below:

- In the MOTOTRBO CPS codeplug tree view, right click on the Connect Plus zone folder and choose “copy”.
- In the MOTOTRBO CPS codeplug tree view, right click on the “Channels” folder and select “Paste”. This will place the copied zone and its 16 identical channels in the “Channels” folder. The radio now has 2 Connect Plus zones, each with 16 identically programmed channels.
- Repeat this process for each additional Connect Plus zone that is needed. The Display Portable and Display Mobile support a maximum of 16 Connect Plus zones. For the Non-Display Portable and the Numeric Display Mobile, the total number of zones is two (Connect Plus and Non-Connect Plus).

The final step will be to assure that Connect Plus zones are at the top of the Channel list as described in the next section.

4.9.5.5 Connect Plus Zone Placement within the Channel List

The last thing to be done is to assure that all Connect Plus zones are at the top of the Channel List. The reason for holding this step until last is that MOTOTRBO CPS automatically places newly created zones as the bottom of the list. For this reason, it makes sense to add all necessary Connect Plus zones prior to rearranging the Channel List.

This section provides guidelines for assuring that the Connect Plus zones are at the top of the Channels List.

For new “out of the box” radios

If a radio is a new, “out of the box” unit, it will likely have one default, non-Connect Plus zone at the top of the list. Edit this zone to make it the first Connect Plus zone by following the instructions in the section, “Creating a Connect Plus Zone and Channel”.

For radios with pre-existing Non-Connect Plus zones

It is possible that the radio may have pre-existing non-Connect Plus zones which should be retained. This may be case, for example, when a conventional MOTOTRBO radio is converted to Connect Plus, and the programmer desires to retain the conventional channels.

If instructions have been followed correctly to this point, the first zone in the list will be a Connect Plus zone, but there may be other Connect Plus zones that are interspersed with non-Connect Plus zones. To re-arrange the list order so that all Connect Plus zones precede all non-Connect Plus zones follow this procedure:

1. Select all of the non-Connect Plus zones that precede the Connect Plus zones. To do this, select each non-Connect Plus zone folder by holding down the “Ctrl” key while clicking the folder. If done correctly, each selected folder title will be highlighted with a blue block.

2. Right click while these folders are selected; choose “Copy” from the right-click menu.

3. Right Click the folder labeled “Channels” at the top of the Channel List. Select “Paste” from the Right Click Menu.

4. This will paste a copy of the selected folders below the Connect Plus folders. At this point, there are two copies of these folders – the originals are still above the Connect Plus folders, and the copies are now below the Connect Plus folders. Verify this before proceeding to the next step.

5. As stated previously, all Connect Plus zones must precede any non-Connect Plus zones. However, after following the instructions to this point, there may be non-Connect Plus zone folders that precede Connect Plus zone folders in the Channels List. If so, edit the non-Connect Plus zone folders to make them into Connect Plus zones. This can be done by deleting all analog channels (if any) in the zone folder and by adding or deleting digital channels so that the total number of digital channels is exactly 16. The digital channels must be identically configured with the settings discussed in the section, “Connect Plus Channel Settings”. It may be necessary to edit the digital channels to achieve this. It is also recommended to rename the zone folder to clarify that it is now a Connect Plus zone.

6. Finally, if there are too many Connect Plus zone folders (either more than desired, or more than the maximum supported number of 16), delete the extra zone entries starting from the **last Connect Plus zone** and working up. The remaining Connect Plus zones can be renamed appropriately.

After following these instructions, all Connect Plus zone folders should be at the top of the Channel List. There will likely be an icon labeled “Channel Pool” that comes immediately after the first Connect Plus zone folder. Any other position for the Channel Pool icon would be unexpected, and would likely result in undesirable operation. If using a CPS version that supports the Zone table view, the first Connect Plus zone must display in the “Position”

Column as position #1. The Channel Pool must display as position #2. If the radio has been configured with additional Connect Plus zones, they must be consecutively numbered, beginning with position #3.

When the programmer has verified that all Connect Plus zones are at the top of the Channel List, then MOTOTRBO CPS programming for Connect Plus is complete. If there is additional programming required for non-Connect Plus operation, it should be finished prior to writing the codeplug to the radio. Once the MOTOTRBO CPS programming is complete, the radio can be programmed with Connect Plus CPS.

4.10 Connect Plus Customer Fleetmap Development

Customer Fleetmap Development for Connect Plus has many similarities to Fleetmap Development for other MOTOTRBO modes, and many of the same processes and principles apply. The primary differences between Fleetmap Development for Connect Plus and other MOTOTRBO modes are as follows:

- In conventional modes, a big part of Fleetmap development is deciding which radios and groups get assigned to which repeater and timeslot. This is not a consideration in a trunking system such as Connect Plus, since the controller assigns channels and timeslots from a common pool on an “as needed” basis.
- In other digital modes, Fleetmap configuration is almost entirely in the subscriber radio (using MOTOTRBO CPS). In Connect Plus, the MOTOTRBO Connect Plus Network Manager and Connect Plus CPS both play a part in Fleetmap configuration. While this adds to the complexity of Connect Plus Fleetmap Development when compared with other modes, it also provides increased management capability and a greater degree of control. For example, in Connect Plus feature access (or feature limitations) can be addressed in two places – in the SU and the Controller. For many features, Connect Plus provides separate controls for the ability to initiate or receive a specific call type. The reader can refer to the section “Connect Plus Features” for description on the Connect Plus feature set.
- For the most part, Connect Plus features are identical or extremely similar to other digital MOTOTRBO modes. Some differences in feature availability that impact Fleetmap Development are that:
    - Connect Plus provides some features not available in other digital modes. These include Multigroup Call, the ability to send a Text Message to a Site All Call ID, and Over-the-air (OTA) File Transfer.
    - Connect Plus does not currently provide some features available in other digital modes.
- In other MOTOTRBO Digital modes, a big part of Fleetmap Development is assigning GPS Revert Channels and/or Data Revert Channels. This is not a consideration in Connect Plus because the controller assigns channels and timeslots for data calls from the same pool of channels used for voice calls. Connect Plus does not use a Control Station radio as the interface between the Connect Plus System and a Location Tracking Application or a Text Message Application. The XRC controller fills this role.
- Scan operates differently in Connect Plus.

4.10.1 Identifying the Needs of Connect Plus Users

Just as in other digital modes, Fleetmap Development begins with identifying who the radio users are, and then identifying the needs of each radio user. Some of the questions that need to be asked include the following:

- Does the radio user have a “preferred site”? In a single site configuration, the “preferred site” is the radio user’s one and only site. In a multisite network, the “preferred site” is the site the radio user will be closest to the majority of time. The radio can automatically Roam from the “preferred site” to other network sites.
- Are there any network sites that the SU should not be allowed to use? If so, the disallowed site(s) should be unchecked in the Site Privileges list on the SU’s user record.

- Is the radio user a supervisor, or not? This impacts which features and privileges are provided to the radio user.

- How important is this radio user when compared to other users? This will determine the user's Priority Level, as configured into the user record in the controller's user database. Because each Talk Group record also has a configurable priority level, this question must be asked for each Talk Group.

- What department or work group does the radio user belong to? Individuals with similar responsibilities and interests are typically assigned to the same Talk Group.

- What other departments or work groups does the radio user need to talk to? This determines which other Talk Groups are programmed into the radio.

- Do a large number of individuals that span multiple departments and work groups share a common trait (such as belonging to the same company or organization)? If so, all of their radios are typically assigned the same Multigroup ID.

- Does the radio user have a need to speak with specific individuals? If so, the radio user should have the ability to initiate Private Calls, and the radio should be programmed with the Private Call destination IDs.

- Does the radio user have a GNSS/GPS and/or Indoor Location capable radio, and is it desirable to track its location? If so, the system must have a Location Tracking Application. The Location Tracking application must be programmed with the IP address and LRRP Port number of the XRC Controller. The application must also be configured with the user's Radio ID and the desired location attributes and update interval.

- Does the radio user have a need to send a text message to a Dispatch PC, or receive a text message from a Dispatch PC? If so, the system must have a Text Message Application. The Text Message application must be programmed with the IP address and TMS Port number for the XRC Controller, and it must also be programmed with the Radio IDs and Group IDs of interest. Both the Text Message Application and Connect Plus SU must be programmed with one or more "Dispatch Call IDs" to represent the Dispatcher Client(s).

- Is the radio user tasked with responsibility for maintaining the radio system? If so, the radio may be programmed with multiple Connect Plus zones, so that the user can monitor and talk to many Talk Groups. Additionally, the radio user may be given the privilege and ability to make a "Site All Call", so that information can be communicated quickly to all site users.

- Does the radio user need to have the ability to transmit an Emergency Alert or Emergency Call request? If so, the radio must be configured for an Emergency button, and the "Emergency Initiation" settings must be configured (all with MOTOTRBO Connect Plus CPS). Furthermore, the unit record for this SU must have the "Emergency Init" checkbox enabled on the user record in the XRC (using the MOTOTRBO Connect Plus Network Manager). If the radio will use a Default Emergency Revert Group ID, then the Group number to be used must be programmed into both the SU and the SU's user record in the XRC.

- Is this radio allowed to send and/or receive a Packet Data Call or Generic Data Call? If so, the Packet Data Call privilege must be enabled in Connect Plus CPS. In the Connect Plus user database, the radio's SU record must be enabled for the appropriate call privilege (Packet Data Call or Generic Data Call).

- Is the radio user equipped with a display radio, and does this radio need to give special ergonomic indications upon receiving an Emergency Call? If so, the "Emergency Call Receive" settings must be configured using MOTOTRBO Connect Plus Option Board CPS.

- Is the radio user equipped with a display radio, and does this radio need to give special ergonomic indications upon receiving an Emergency Alert? If so, the “Emergency Alert Receive” settings must be configured using MOTOTRBO Connect Plus Option Board CPS.

- Does the radio user need to make and/or receive protected transmissions? If so, then Enhanced Privacy must be configured with both MOTOTRBO CPS and Connect Plus CPS. See Section 2.16, Connect Plus Voice and Data Privacy.

The process of identifying radio users and their needs should involve the radio users themselves, both at the management and non-management level. It should also be documented in a database or spreadsheet that can be used as a basis for Fleetmap Development. The database or spreadsheet should contain the following information for each radio user:

- Name
- Work area (which will be mapped to a radio talkgroup)
- Radio Model
    - Is radio GNSS/GPS and/or Indoor Location capable? Are location updates desired?
    - Does radio have a display? (Controller will not allow text messages to SU if no display?
- Radio Serial Number
- Radio Physical Serial Number
- Radio ID
- Multigroup ID
- Default Emergency Revert Group
- Other Talk Groups the user will communicate with
- What Priority is this radio user? Each Connect Plus user record and Group record has a programmable Priority Level, 2-8. Priority 2 is the highest configurable level. Priority Level 8 is the lowest Priority Level. The Controller considers Priority Level when assigning Calls from the Busy Queue.
- If the radio is configured for Enhanced Privacy, record which Key IDs and Key Values are used on the MOTOTRBO CPS Privacy Table. Also, record TX Key ID assignment per Talk Group as configured with Connect Plus CPS.
- Feature Privileges
    - Receive Private Calls?
    - Initiate Private Calls?
    - Initiate Multigroup Call? (voice & text)
    - Initiate Voice Call to Site All Call ID?
    - Send Text Message to Site All Call ID?

- Initiate Remote Monitor for another SU?
- Allow Remote Monitor by another SU?
- Send “Disable Command” to another SU?
- Receive Disable Command sent by another SU?
- Send “Enable Command” to another SU?
- Receive Enable Command sent by another SU?
- Send Radio Check to another SU?
- Send Call Alert to another SU?
- Receive Over-the-Air File Transfer to update Connect Plus Option Board Firmware and Network Frequency File?
- Initiate Emergency Alert or Emergency Call?
- Send and/or receive a Packet Data Call or Generic Data Call?
- Are there any network sites that the SU should not be allowed to use?

As the process evolves, it is not unusual to discover that individuals and needs fall into several general categories. Each of these categories may evolve into its own codeplug template.

4.10.2 Important Information about Connect Plus Call Initiation Privileges

The XRC Controller provides several programmable Call Initiation Privileges for each SU record. Once an SU is enabled with a privilege (such as the “Private Call Init” privilege) the XRC Controller does not maintain a list of which SU’s that specific radio is allowed to call. Which SU’s the radio can call is determined by the following:

- If Manual Dial is NOT enabled in the radio via Connect Plus CPS, the radio can attempt to call any Private Call ID on its Zone Contact List.
- If Manual Dial is enabled in the radio via Connect Plus CPS, the radio can attempt to Private Call any Private Call ID entered via the keypad. This essentially means that the SU can attempt to call any Private Call ID network-wide.
- When the SU attempts to initiate a Private Call, the XRC Controller will allow the radio to call any SU that has the “Private Call receive” privilege enabled on its user record in the controller database.

The same principles also apply to Remote Monitor, Radio Check, Call Alert, Radio Disable, and Radio Enable.

4.10.3 Who will the Connect Plus radio user hear?

The Connect Plus radio can receive one call at a time. While the radio is receiving one call (either voice or data), it’s possible that radio will not hear part or all of another call that it would otherwise respond to.

Assuming that the Connect Plus radio is idle and monitoring its Control Channel, the SU will respond to any of the following call assignments on a first-come first-served basis.

- The SU will respond to a call targeting its individual ID. This includes Private Calls, Call Alert, Radio Check, Remote Monitor, Radio Disable, Radio Enable, Text Message to the individual ID, Location Update Request. If it is not desirable for the radio user to receive one of these call types, then the SU record in the controller database should not be configured with the corresponding “receive” privilege.

- The SU will respond to a call targeting its Selected Group ID. The Selected Group ID is the Group ID currently selected with the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio). Or, if a Private Call ID is currently selected on the Channel Selector Knob or Channel Rocker, the SU will respond to the “Registration Group ID” that has been programmed for that Knob or Channel Rocker position. Call types include voice call to the Group ID or text message to the Group ID.

- The SU will respond to a call targeting its Multigroup ID. The user’s Multigroup ID is configured in two places; in the subscriber radio and in the user record in the controller database. Call types include voice call to the Multigroup ID or text message to the Multigroup ID.

- The SU will respond to a call targeting the Site All Call ID. This includes Site All Call (voice) initiated by another radio using the same site, or Network Wide All Call (voice) initiated by a device (such as a wireline digital console) that connects to the Connect Plus network via the XRT Gateway. The radio also responds to text messages received on the Site All Call Text ID.

4.10.4 Who will the Connect Plus radio user talk to?

For the purposes of this discussion, the expression “talk to” will be used in a broad sense to include both voice and data features.

Who the Connect Plus radio user can “talk to” is determined by several factors:

- What privileges are configured into the controller’s user database? Whenever the user record provides a programmable privilege, it always takes precedence over how the radio has been programmed with Connect Plus CPS. For example, the radio may be configured with the Menu option to initiate Remote Monitor. However, if the “Remote Monitor Init” privilege is not enabled on the user record in the controller database, the radio’s request to start a Remote Monitor will be denied.

- How has the radio been programmed with Connect Plus CPS? SU programming and controller programming should be in synch in regards to the SU’s privileges. If the radio user is not allowed to Remote Monitor other SU’s, then the “Remote Monitor Init” privilege should not be enabled in the controller’s user record and the radio should not be programmed with the Remote Monitor menu option.

- What Talk Groups have been assigned a position on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio)?

- What Multigroup ID has the radio been programmed with? Has the Multigroup ID been assigned a position on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio)? This is required for the radio to initiate a voice call to the Multigroup ID. Has the user record in the controller database been enabled for the “Multigroup Call Init” privilege?

- Has the Site All Call voice ID been assigned a position on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio)? This is required for the radio to initiate a voice call to the Site All Call ID. Has the user record in the controller database been enabled for the “Site All Call Init” privilege?

- Does the radio have a display? If not, the ability to initiate calls is restricted to calls assigned to a Channel Selector Knob (portable radio) or Channel Rocker (mobile radio) position, or programmed “One Touch Calls”. If the radio does have a display, what Menu options have been configured? This determines which calls can be initiated via the radio menu.

- Has the radio been programmed with the ability to do One Touch Calls? If so, what call types and Destination IDs have been programmed for the One Touch Call(s)? In Connect Plus, One Touch Call can be used to initiate the following Call Types:

  - Private Call (voice call) to a specific Destination ID

  - Call Alert to a specific Destination ID

  - Programmed “Quick Text” Message to a specific Destination ID. The Destination ID can be either an individual (Private Call) ID or a Group ID.

- Does the radio have a keypad (and therefore the ability to “Manually Dial” an individual ID)? If the radio doesn’t have a keypad, or if it does have a keypad but “Manual Dial” hasn’t been enabled as a Menu option, then the only individual IDs that can be targeted for calls will be those on the radio’s Contact List. Group IDs cannot be entered via Manual Dial.

4.10.5 Assigning Connect Plus Radio IDs

Each Connect Plus radio user must be assigned a unique Radio ID between 1 and 16776351. The Radio ID used for each mobile or portable SU must be unique network wide. The only exception to this rule is for repeater Radio IDs. The assignable range for repeater Radio ID’s is 1-15. Each repeater at a site must have a unique Radio ID, but the same Radio ID can (and probably will) be used again for another repeater at a different site.

Because such a wide range of assignable Radio ID’s are available for Connect Plus SU’s, the Network Administrator has many possible strategies to choose from when assigning a radio its Radio ID. The following are just some examples:

- If “Manual Dial” (direct entry from the radio keypad) will be used as a strategy for making individual calls, this would be a good reason for making Radio IDs as short as possible.

- Radio ID’s may be assigned so that each number in the Radio ID represents something. The first digit may represent the type of radio (mobile vs. portable), the second digit might represent a department, the next three digits might represent the user, and so forth.

- Radio Users in the same company or department might be assigned from the same contiguous ranges. For example, Department A radios may be assigned from the range of 100 to 199, Department B from 200 to 299, etc.

- It may be helpful to plan for a relationship between a Group ID and the Radio ID’s of the users of that Group. For example, Talk Group A may use Talk Group 1000 and their Radio ID’s may be assigned from the ranges of 101 to 199. Talk Group B may use Talk Group 2000 and their Radio ID’s may be assigned from the ranges of 201 to 299. While it is allowable to use the same number as both a Radio ID and Talk Group ID, it is not recommended due to the confusion it may create and the availability of large number of ID’s. Using different numbers for Groups and Radio ID’s can help the radio user and System Administrator differentiate quickly between Group IDs and individual IDs. For example: Talk Group IDs may end with 00, while the radios in the fleet could have the last two digits between 01 and 99, as in the following radio ID assignments:

  - Talk Group IDs: 1000, 1100, etc; SUIDs: 1001 – 1099, 1101 – 1199, etc.

- Some Network Administrators like to match Radio IDs with vehicle numbers. It should be noted that if a single radio user has two radios – both a portable and mobile, for example – the two radios must have different radio ID's. However, the Network Administrator can plan for a relationship between the two numbers. For example, the mobile radio in "Joe's" vehicle might be Radio ID 50, while "Joe's" portable radio is assigned Radio ID 150.

The Radio ID is programmed into the SU with MOTOTRBO CPS. See the section, "Setting the Connect Plus Radio ID" for important information on configuring the Connect Plus Radio ID with Connect Plus CPS.

Each XRC Controller in the network must have an identical user record for each Connect Plus Radio ID. Connect Plus helps the Network Administrator fulfill this rule in two ways:

- Whenever a user record is added to the user database at any Connect Plus site (or an existing record is updated with revised information), the site will automatically forward a copy of the record to other network sites. This is done on a record-by-record basis after the programmer makes the desired changes and then saves the record.

- If a new Connect Plus site is brought on-line the Network Manager software makes it easy to copy the entire user database from an existing Connect Plus site to the new site.

In case when merging of two or more Connect Plus systems is expected in the future helpful guidelines on Radio ID assignments have been provided in Appendix C.

4.10.6 Assigning Aliases for Connect Plus Radio IDs

Connect Plus CPS can be used to assign aliases for Connect Plus Radio IDs. For example, "Fred's radio" can be programmed to know that "Sue" has Radio ID 250. This is helpful in a couple of ways:

- When "Fred" wants to make a call to "Sue", he can simply choose "Sue" from the Contact List. This assumes that Fred's radio has been programmed with a Private Call Contact for ID 250, and that "Sue" has been entered as the "Contact Name" for the contact record.

- When "Fred" receives an individual call from "Sue" (or when "Sue" transmits during a Group Call), his display will show "Sue", rather than Sue's Radio ID. This assumes that Fred's radio has been programmed with a Private Call Contact for ID 250, and that "Sue" has been entered as the "Contact Name" for the contact record.

While the two features described above are convenient for "Fred", a word of caution should be mentioned. If something happens to where Radio 250 no longer belongs to Sue, this is a problem because "Fred's" radio will continue to display ID 250 as "Sue". Changing the alias on the contact record can be performed either by reprogramming the radio with the updated Option Board codeplug or manually editing the contact through the subscriber menu.

For this reason, some Network Administrators avoid using a person's name as the "Contact Name" for a contact record. In place of the individual's name, they prefer to use a job title, vehicle name or number, etc.

Some Network Administrators prefer not to program Private Call contacts at all. In this case, the radio will display the Call ID in place of the alias for incoming transmissions. Also in this case, "Manual Dial" would be the only option for initiating individual call types. The radio requires a keypad to support "Manual Dial".

If Private Call contact records and aliases are used, all radios should be programmed in a consistent manner so that the alias information in "Radio A" will be the same as the alias information in radios "B", "C" and "D".

It should also be noted that the user record in the Connect Plus controller has a field called "alias", but this alias is not transmitted over the air and it has no effect on what appears on a radio's display. The alias on a radio's display is determined via Contact List programming with Connect Plus CPS.

4.10.7 Assigning Connect Plus Group IDs

A Group Call allows multiple radios to participate in the same conversation.
Therefore, the organization of Group IDs is one of the most important decisions that will be made during the Fleet Mapping process. In most cases, a Group ID represents a department or work group. However, this merits a note of caution. While every department might desire its own ID for Group communications, this may not be advisable for several reasons:

- The more different Group IDs that have been assigned to radios, the busier the site and network is likely to be.

- The more different Group IDs that are programmed into any individual radio, the easier it is for the radio user to get "lost in the radio" and miss important communications because he/she is selected to the wrong group.

For this reason, it is advisable for multiple departments or work groups to share a common Group ID wherever possible.

The assignable range for Connect Plus Group ID's is 1 to 16776351. Once a Talk Group ID has been selected for a work group or department, the number should not be assigned to any other Group (or Multigroup) network-wide. While it is allowable to use the same number as both a Radio ID and Talk Group ID, it is not recommended due to the confusion it may create and the availability of large number of ID's. Using different numbers for Groups and Radio ID's can help the radio user and System Administrator differentiate quickly between Group IDs and individual IDs.

In case when merging of two or more Connect Plus systems is expected in the future helpful guidelines on Group ID assignments have been provided in Appendix C.

4.10.8 Programming Connect Plus Group IDs

A Group ID record that matches the Group number selected for the work group or department must be programmed into the XRC controller. Just as with the individual record for Radio IDs, the controller will automatically send the Group record to all of its connected sites.

Additionally, the Group ID must be programmed into the radio of each Group member using Connect Plus CPS. The following bullets describe the required steps:

- In each Connect Plus zone that requires the Group ID, use Connect Plus CPS to create a "Group Call" contact record with the "Call ID" and the "Contact Name". The "Contact Name" typically describes the work group or department (such as "shipping" or "security").

- After the Group Call Contact Record has been created, it must be assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio), using the Connect Plus CPS Zone Channel Selections Screen. For each position (up to a maximum of 16 positions), there are three programmable fields; "Contact Name", "Registration Group Name" and the "RX Only" checkbox. The "Contact Name" field is used to program which Group Call will be started when the radio is selected to that position and PTT is pressed. When the "Contact Name" is programmed with a Group Call, the

software automatically programs the “Registration Group Name” field with the same Group Call info. The “RX Only” checkbox should be checked if the radio user is allowed to listen to the group only, but is not allowed to transmit.

4.10.9 Making a Group Call

To start a call to the Group, the radio user selects the Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) that has been programmed for the desired Group. If the knob or channel rocker has been changed from a different position, the radio will automatically re-register with the newly selected Registration Group. Following the registration, the radio user may press PTT to start the call. When the radio sounds the “Talk Permit” tone, a timeslot has been assigned and the user may proceed to talk while pressing PTT. The transmission will be heard at any network site that has at least one radio registered to the Group, or where the Group is permanently registered, and where there is an available repeater timeslot for call assignment. When the radio user releases PTT, the repeater starts the Group Call Hang Time. This allows other individuals in the Group to speak without having to initiate a brand new call.

Each transmission is identified with two numbers; the Group ID number and the Radio ID of the transmitting radio. The Group ID is what allows multiple radios to hear the same transmission. The Radio ID allows the receiving radios to know which individual within the Group is currently transmitting.

It is important to note that Group voice calls cannot be initiated via the radio menu or by pressing a “One Touch Call” button in Connect Plus. In order to start a Group voice call, the user must select the programmed position on the Channel Selector Knob (portable) or Channel Rocker (mobile).

4.10.10 Assigning Connect Plus Multigroup IDs

A Multigroup ID is a special type of Connect Plus Group feature that does not exist in other MOTOTRBO digital modes.

Each Connect Plus radio can be programmed with one Multigroup ID. The Multigroup ID is programmed into the radio using the **Networks** screen of Connect Plus CPS. This same number must be programmed into the Multigroup ID field of the user record corresponding to the SU in the controller's user database.

Multigroup operation differs from regular Connect Plus Groups in several important ways:

- The radio user doesn't need to select the Multigroup in order to hear transmissions on the Multigroup ID. Regardless of which Group is currently selected via the Channel Selector Knob position (portable radio) or Channel Rocker (mobile radio), the radio automatically listens for Multigroup transmissions also.

- Because a radio's Multigroup ID is programmed into its unit record in the controller's database, the Connect Plus radio doesn't need to register with the Multigroup ID. The radio registers with its selected Group, and the controller automatically registers the radio to both its Selected Group and its Multigroup. This allows the radio user to hear Multigroup transmissions no matter which site he/she is registered to, and no matter which Talk Group is currently selected. If the Multigroup ID happens to also be the selected Group ID, then the radio does register with the Multigroup ID.

- A radio user requires a programmable privilege to initiate a Multigroup transmission. The "Multigroup Init" privilege is kept on the user record in the controller's user database. This permission is checked when (a) starting a voice call to the Multigroup ID, and (b) sending a text message to the Multigroup.

- A Multigroup voice call is a one-way transmission. The repeater starts the Group Hang Time after the transmission, but only the call initiator is allowed to talk during the Group Hang Time. If another radio wishes to transmit on the Multigroup, it will be processed as a new call request, and the call initiator must have the programmable permission. For this reason, the Multigroup is well suited for announcements to large numbers or radios, but it is not designed to be a conversation group.

- If the system designer/administrator does not want to include an SU in any Multigroup call, then the SU should not be assigned a Multigroup ID.

In order for a radio to hear a Multigroup transmission, all of the following requirements must be met:

- The matching Multigroup ID must be programmed into the subscriber via the Connect Plus CPS Networks screen.

- The radio must be registered to the site and monitoring the Control Channel downlink in order to receive the call assignment. If a radio is involved in a previous call on another trunk-to timeslot, it may miss all or part of the Multigroup Call.

Deciding which SU's will share the same Multigroup ID is an important Fleet Mapping decision. Since the Multigroup works best as an announcement group, an important factor is deciding whether a large group of users shares a common interest – such as belonging to the same company or organization. If so, it makes sense to place them in the same Multigroup.

The assignable range for Connect Plus Multigroup ID's is 1 to 16776351. Note that this is the same range used for regular Talk Groups. Any number from this range can be assigned to a regular Talk Group or a Multigroup ID, but not both. Once a number has been used as either a Talk Group or Multigroup, it cannot be used again.

In case when merging of two or more Connect Plus systems is expected in the future helpful guidelines on Multigroup ID assignments have been provided in Appendix C.

4.10.11 Programming Connect Plus Multigroup IDs

4.10.11.1 Placing Multiple Radio Users in the Same Multigroup

Placing multiple radio users in the same Multigroup is simply a matter of assigning them the same Multigroup ID. To assign a Multigroup ID, use the following steps:

- Create a Multigroup record for the ID in the controller's user database. Just as with other subscriber records, the controller will automatically send the Multigroup record to all of its connected sites.
- Also in the controller user database, program the Multigroup ID into the "Multigroup ID" field on the unit record for each SU that will be a member of the Multigroup.
- When programming subscriber radios, each radio in the Multigroup should be programmed with this Multigroup ID. The set of radios that is programmed with "Multigroup ID X" should match the set of user records that have been programmed with the same Multigroup ID.
- A radio doesn't need to be programmed with a Multigroup contact record in order to receive a Multigroup call. This is because the Multigroup ID is programmed on the Connect Plus CPS Networks screen. The contact record is required for the following:
    - To display a programmable alias for the Multigroup ID.
    - To assign a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) to the Multigroup ID. Assigning a Knob or Rocker position is required to initiate a Multigroup Call, but not to receive a Multigroup Call.

4.10.11.2 Programming for Multigroup Call Initiation

To allow a radio user to initiate a Multigroup Call, the following steps are required:

- In the controller database, check the "Multigroup Init" checkbox on the user record corresponding to the SU that should have the privilege.
- In each Connect Plus zone that requires call initiation on the Multigroup ID, use Connect Plus CPS to create a "Multigroup Call" contact record with the "Call ID" and the "Contact Name" for the Multigroup.
- After the Multigroup Call Contact Record has been created, it must be assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio), using the Connect Plus CPS Zone Channel Selections Screen. The procedure for assigning a programmable Knob or Rocker position is the same as described previously for a Group Call, except that the Multigroup ID is assigned as the Contact Name.

4.10.12 Making a Multigroup Call

The procedure for starting a Multigroup Call is the same as for starting a Group Call. Prior to granting the call request the controller will check to see if the initiating radio has the "Multigroup Init" privilege on its unit record in the controller's user database.

When the radio user releases PTT after a Multigroup transmission, the repeater starts the Group Call Hang Time. Unlike other Group Calls, only the call initiator can transmit again during the Call Hang Time.

It is important to note that Multigroup calls cannot be initiated via the radio menu or by pressing a "One Touch Call" button. In order to start a Multigroup Call, the user must select the programmed position on the Channel Selector Knob (portable) or Channel Rocker (mobile), and the user record must be configured for the programmable "Multigroup Init" permission in the controller's user database.

4.10.13 Site All Call ID

The Site All Call ID in Connect Plus is very similar to the All Call ID in other MOTOTRBO digital modes. The word "Site" is added in Connect Plus to emphasize that these transmissions are heard only at the site where the call initiator is located. Unlike other Connect Plus Calls, audio is NOT networked beyond the originating site, and therefore radio users registered at remote sites or wireline console operators will never hear a radio-initiated Site All Call. In Connect Plus, an authorized user can also send a Site All Call Text Message. The Text Message will only be transmitted at the originating site. It will not be networked to other sites.

Note: Although a radio-initiated Site All Call is not networked beyond the originating site, a Network Wide All Call (NWAC) utilizes the Site All Call ID and is networked to multiple sites. NWAC is initiated by a device (such as digital a wireline console) that connects to the Connect Plus network via the XRT Gateway. NWAC cannot be initiated by a subscriber radio. When a radio receives a NWAC, it is displayed on the receiving radio as a Site All Call. For more information, see the section "Network Wide All Call".

4.10.13.1 Site All Call Differences

Site All Call differs from other Connect Plus Groups in several important ways:

- It is not necessary to create records for the Site All Call in the controller's user database. This is because the controller is "hard coded" with information about the Site All Call IDs. These records cannot be viewed or edited.
    - Site All Call (voice) uses a fixed ID of 16777215. This cannot be changed by the user.
    - Site All Call (text) uses a fixed ID of 16776415. This cannot be changed by the user.
- The radio user doesn't need to select Site All Call in order to hear transmissions on the Site All Call ID. Regardless of which Group is currently selected via the Channel Selector Knob position (portable radio) or Channel Rocker (mobile radio), the radio automatically listens for Site All Call transmissions also.
- A radio user does not have to register with the Site All Call ID to hear Site All Call transmissions.
- A radio user requires a programmable privilege to initiate a Site All Call transmission. There are separate permissions for "Site All Call Voice Init" and "Site All Call Text Init". These permissions are kept on the user record in the controller's user database.

- A Site All Call voice call is a one-way transmission. There is no Group Hang Time after a Site All Call transmission. If another radio wishes to transmit on the Site All Call ID, it will be processed as a new call request, and the call initiator must have the programmable permission. Site All Call should only be used for important announcements of interest to all site users. It is not a conversation group.

In order for a radio to hear a Site All Call transmission, the radio must be registered to the site and monitoring the Control Channel downlink in order to receive the call assignment. If a radio is involved in a previous call on another trunk-to timeslot, it may miss all or part of the Site All Call.

Deciding which individuals can initiate a Site All Call is an important Fleet Mapping decision. In many networks this privilege is only granted to the individual responsible for maintaining the site and/or network. Once a radio user has been granted the permission, he/she should also be educated about how and when to use the Site All Call ID. Because Site All Call transmissions are heard by all idle radios registered to the site, they can be disruptive to normal communications.

4.10.13.2 Enabling Radio to Initiate a Site All Call

To allow a radio user to initiate a Site All Call, the following steps are required:

- In the controller database, check the “Site All Call Voice Init” and/or the “Site All Call Text Init” checkbox(es) on the user record corresponding to the SU that should have the privilege(s).

- In each Connect Plus zone that requires call initiation on the Site All Call ID, use Connect Plus CPS to create a “Site All Call” contact record. Note that there are separate record types for “Site All Call Voice” and “Site All Call Text”. Only “Site All Call Voice” can be assigned a position on the Channel Selector Knob (portable radio) or Channel Rocker (mobile radio).

- After the Site All Call Voice Contact Record has been created, it must be assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio), using the Connect Plus CPS Zone Channel Selections Screen. The procedure for assigning a programmable Knob or Rocker position is the same as described previously for a Group Call, except that the Site All Call Voice Contact is assigned as the Contact Name. Also, when Site All Call Voice is assigned as the Contact Name, any type of Group Record can be assigned as the Registration Group Name. The advantage of assigning a different Group Call as the Registration Group Name is that it allows the radio to also receive calls on that ID while selected to the “Site All Call Voice” position.

4.10.14 Making a Site All Call

The procedure for starting a Site All Call is the same as for starting a Group Call. Prior to granting the call request the controller will check to see if the initiating radio has the “Site All Call Voice Init” privilege on its unit record in the controller’s user database.

When the radio user releases PTT after a Site All Call transmission, the repeater does not enter the Call Hang Time. Instead, the call ends immediately and all radios return to the Control Channel timeslot.

It is important to note that Site All Call voice calls cannot be initiated via the radio menu or by pressing a “One Touch Call” button. In order to start a voice Site All Call, the user must select the programmed position on the Channel Selector Knob (portable) or Channel Rocker (mobile), and the user record must be configured for the programmable “Site All Call Voice Init” permission in the controller’s user database.

4.10.15 Network Wide All Call (NWAC)

NWAC is a one-way voice transmission initiated by a device (such as a digital wireline console) that connects to the Connect Plus network via the XRT Gateway. The device acts as an XRC Client. NWAC cannot be initiated by a subscriber radio. NWAC is a best-effort service that utilizes the Site All Call ID (16777215). NWAC is transmitted at every network site that has an available RF resource and where the ID is not already in use. The NWAC transmission is placed on the air even if there are no radios currently registered to the site.

Depending on resource availability, it is possible that the NWAC may be placed on the air at some sites and placed in Busy Queue at other sites. If the NWAC transmission is still in-progress when a voice channel becomes available, the NWAC will be assigned from the Busy Queue. (NWAC is assigned from the Busy Queue according to the configured priority level on the call initiator's user record.) Radios at that site which are not already engaged in a call will hear the remainder of the NWAC transmission as late-joiners. If the NWAC transmission ends before a voice channel becomes available, the NWAC will be removed from the Busy Queue.

If a radio is currently transmitting a Site All Call when the XRT Client initiates a NWAC, the XRT Client NWAC transmission will not be heard at that site. In this scenario, the NWAC is not placed in the Busy Queue. Networks that utilize NWAC may wish to disable the Site All Call Voice Initiation privilege for Connect Plus radios. This will prevent the potential conflict between the radio-initiated Site All Call and the XRT Client-initiated NWAC.

When a radio receives a NWAC, it is displayed on the receiving radio as a Site All Call. Just as with Site All Call, the radio does not require any special programming to receive a NWAC. It always responds to a NWAC, provided that it is not already involved in another call when the NWAC starts. If the radio is involved in another call when the NWAC starts, it will join the NWAC when the previous call ends (provided that the NWAC is still in-progress). There is no Call Hang Time at the end of a NWAC transmission.

NWAC is shown on the Network Manager Real Time Display as Network Wide All Call. NWAC is logged in the Airtime Log as Network Wide All Call.

Note: A Connect Plus radio does not have to register the Site All Call ID in order to receive either a Site All Call or a Network Wide All Call. However, a XRT Client (such as a digital wireline console) cannot initiate or receive a NWAC unless it has registered the special Talk Path ID of 16777215 with the XRT Gateway. In order to register this special Talk Path ID, the XRT Client must be configured for "NWAC Enabled" with the XRT Configuration Tool (*Settings → XRT User Configuration*). If the XRT Client has registered this special Talk Path ID, it can receive a NWAC initiated by another Client that is connected to a different XRT. However, the XRT Client will never hear a radio-initiated Site All Call because a Site All Call is not networked beyond the originating site.

4.10.16 Connect Plus Private Calls

Private Call refers to the ability for one individual radio user to call another individual radio user regardless of whether the units share any common Talk Groups. The voice communication takes place using the Private ID's (individual Radio ID's) of the two units. So, the term "Private" means that the call involves two individual ID's, the source and destination. It does not mean that the voice packets are encrypted in any special way.

In other digital modes, Private Calls can be configured as "confirmed" or "unconfirmed" based on MOTOTRBO CPS programming. In Connect Plus, a Private Call always requires a Control Channel acknowledgement from the destination SU before the controller will assign a trunk-to timeslot. In this sense, Connect Plus Private Calls are always confirmed. However, the "Private Call Confirmed" checkbox must not be enabled for any Connect Plus channel via MOTOTRBO CPS. This requirement prevents the participating radios from performing an additional and unnecessary CSBK exchange on the trunk-to timeslot prior to transmitting voice.

In Connect Plus, the privilege to “initiate” a Private Call and the privilege to “receive” a Private Call are separate programmable privileges on the unit record in the controller’s user database. One of the most important Fleet Mapping decisions is whether an individual should be given one or both of these privileges.

Giving many users the ability to initiate Private Calls is somewhat risky for several reasons:

- Some radio users may “hide out” in private conversations so as not to be monitored by the supervisor or Group members.
- In a related issue, a user can miss important Group communications while on a Private Call.
- If many users make Private Calls, the system will get very busy. This is because each Private Call captures at least one repeater timeslot. If the parties are located at different sites, the Private Call uses a repeater timeslot at each site.

On the other hand, if Private Calls are conducted in an educated manner, they can actually save system resources. For example, “Molly” and “Maria” are both members of the “Transportation” Talk Group, which currently has Talk Group members registered to five different sites. Molly needs to discuss some company business with Maria that is otherwise unrelated to the Transportation Talk Group. If Molly were to conduct this conversation on the Transportation Talk Group, the call would use five different repeater timeslots – one at each registered site. However, if Molly makes a Private Call to Maria, she can avoid tying up the Talk Group, and the call will only use a maximum of two repeater timeslots. If Molly and Maria are registered to the same site, the Private Call will only use one repeater timeslot.

In order for a Connect Plus Private Call to take place; all of the following must occur:

- The Source ID must be enabled for the “Private Call Initiation” privilege on its SU Record in the controller database,
- The Destination ID must be enabled for the “Private Call Receive” privilege on its SU Record in the controller database,
- The Destination SU must be registered to a network site and not currently busy in a call
- The Destination SU must acknowledge a Control Channel query before the controller will assign a trunk-to timeslot for the call. This acknowledgement is provided automatically by the destination radio. The radio user is not aware of the incoming Private Call until the trunk-to timeslot is assigned.

Private Calls are message trunking. At release of PTT the assigned trunk-to timeslot enters the Private Call Hang Time. During the Private Call Hang Time, either party may transmit on the same trunk-to timeslot. If the Hang Time expires with no further transmissions the call ends.

4.10.17 Initiating a Private Call in Connect Plus

Just like other MOTOTRBO digital modes, Connect Plus provides several different ways to initiate a Private Call. The number of ways available to any particular individual depends on his/her radio model:

- Select a Private ID from the Contact List and press PTT. This is the most common way to initiate a Private Call, but it is only available to display radios.
- Place the radio in “Manual Dial” mode, and then enter the destination Private Call ID via the keypad and press PTT to start the call. This method is only available to display radios with a keypad.
- After receiving a Call Alert, press PTT while the “ignore?” prompt still shows on the radio display. This will initiate a Private Call to the radio that sent the Call Alert.
- Initiate a Private Call via a pre-programmed One Touch Call button. This can be used to initiate a Private Call to a specific, pre-configured destination ID. This approach is available to all radios.
- Initiate a Private Call by assigning a programmable Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) to a Private Call ID. Then select the assigned position and press PTT to start the Private Call. This approach is available for all radios, but it is more common for non-display or numeric display radios, which don’t have the option of initiating Private Calls via the Menu. The specific steps for this approach are as follows:
    - In each Connect Plus zone, use Connect Plus CPS to create a “Private Call” Contact record for each Private Call destination ID that will be assigned a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio).
    - After a Private Call contact record has been created, it should be assigned to a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) using the Connect Plus CPS Zone Channel Selections Screen. The procedure for assigning a programmable Knob or Rocker position is the same as described previously for a Group Call, except that the destination Private Call ID is assigned as the Contact Name. Also, when a Private Call is assigned as the Contact Name, any type of Group Record can be assigned as the Registration Group Name. The default Registration Group Name in this case is the Site All Call Voice ID, but it is highly recommended to change this to a different Group. In doing so, it is advisable to use a Group that is not the Site All Call Voice ID or the Multigroup ID. The radio will still receive calls on these two ID’s, even they aren’t programmed as the Registration Group. So, it’s to the user’s advantage to program a different Registration Group. If the user were to accidentally leave the Knob or Channel Rocker in this position after the Private Call ends, the user would hear communications on the programmed “Registration Group” (in addition the Multigroup ID and the Site All Call Voice ID).

4.10.18 Configuring Priority Levels in Connect Plus

Every Call Request received by the XRC controller has a Source ID and a Destination ID. The Source ID tells the controller which SU is initiating the call. The Destination ID tells the controller whether the call is targeted to another SU or to a Group ID. Both the Source ID and the Destination ID have a corresponding record in the controller’s user database, and each of these records has a programmable Priority Level (2-8). Two is highest configurable Priority Level, and 8 is the lowest configurable Priority Level. These Priority Levels come into play when there is no trunk-to timeslot available, and the Controller must place the call into the Busy Queue.

When a timeslot becomes available, the Controller assigns the highest priority call from the Busy Queue. Emergency Calls have the highest priority, followed by Emergency Location Update. If there are no Emergency

Calls to assign, the controller assigns non-emergency calls based on the configurable priorities of the IDs involved in the call. In doing so, it considers the Priority Level of both the Source ID and Destination ID. As a general rule, the call is assigned from the Busy Queue according to the higher of the two priorities. Site All Call requests are prioritized according to the priority of the Source ID only. A Network Wide All Call request (which can only be made by a non-radio device such as a digital wireline console) is handled the same as a Site All Call request. When priority levels are equal, the Controller considers other factors when deciding which call to assign from the Busy Queue:

- For calls of equal priority, voice calls have priority over data calls.
- For voice calls of equal priority, calls are assigned “first in, first out”.
- For data calls of equal priority, calls are assigned “first in, first out”.

An important part of Fleet Map Design is determining which Priority Level will be assigned to each radio user and to each Talk Group. The Priority Level will then be configured into the corresponding record in the controller’s user database. One simple approach is to leave every Talk Group record at the default Priority Level of 8 (the lowest Priority). In this approach, all Talk Groups are equal priority. Therefore, Group calls will be assigned from the Busy Queue based on the Priority Level of the Source radio only. Where priorities are equal, the calls will be assigned “first in, first out”.

4.10.19 Text Messaging Considerations for Fleet Mapping Design

Connect Plus supports Simple Text Messaging as alternative to voice communications, and text messaging capability should be considered during Fleet Map design.

The system designer should be familiar with Connect Plus Text Messaging features as discussed in the System Feature Overview Section. In addition, some other Text Message considerations are as follows:

- While all Connect Plus radio models have voice capability, some Connect Plus radio models have very limited text message capability. Non-display and numeric display radios cannot receive a text message, and they can only send pre-programmed (quick text) messages that are mapped to specific Destination ID via the “One Touch Call” feature.
- The amount of information that can be carried in a single text message is 138 to 280 characters, depending on the source and destination devices for the message.
- For text messages to an individual ID, the initiating radio sends the message to the controller, which places the message in the mailbox for the destination SU. The controller will deliver the message to the destination SU at the earliest opportunity, but this is subject to (a) SU availability and (b) timeslot availability. If the SU is not currently registered into the network, the controller will hold the message until the SU registers, or until the message times out. If the text message cannot be delivered prior to the “Text Message Retention Timer” timeout period (configurable in the XRC Controller), the message will be deleted.
- Each SU has a mailbox in the XRC controller, and each SU mailbox can hold 10 undelivered messages. If the controller cannot deliver messages due lack of SU availability (because the SU is not registered into the network, for example), and if the mailbox fills up, the controller will not accept any more messages for the SU. If a radio user tries to initiate a text message to an SU when its controller mailbox is full, the call request is denied due to “Destination Mailbox Full”. Because the controller did not accept the message for delivery, the radio user will have to try again at a later time. The mailbox remains full until messages are removed because they are delivered to the Destination SU, or because the text message times out.

- To send a Text Message to an individual ID, the radio user can select the destination Private Call ID from the Contact List, or manually dial the Private Call ID (keypad is required for Manual Dial).

- In order to send a Text Message to a Group ID, the radio must have a Group Call contact record for the destination Group. Direct Dial for Group IDs is not supported.

- There is no mailbox for text messages addressed to a Group. When the controller receives a text message addressed to a Group ID, the controller will transmit the message at each site where the Group is currently registered. Because there is no OTA acknowledgement for Group Text Messages, this is a "best effort" attempt on the part of the controller. The controller will not know for certain which SU's did or did not receive the Group Text Message.

- When a radio receives a text message that was addressed to the Group ID, the radio user will not be aware that it was addressed to a Group and not to the radio's individual ID. This is also true for other MOTOTRBO digital modes. If the user selects "Reply", the reply text message will be addressed to the individual ID that was the source of the Group Text Message, it will not be addressed to the Group ID.

- If a single Group ID includes both display radios and non-display radios (or numeric display radios), voice communications is preferable to text. This is because the non-display and numeric display radios will not be able to display the text messages. If a text message is sent to a Group ID that contains non-display or numeric display radios, all Group radios will move to the trunk-to timeslot, but only the display capable radios will notify the radio user that a Text Message has been received.

- In order to send a Text Message to a Multigroup ID, the source radio must have the "Multigroup Init" privilege enabled on its user record in the controller's user database.

- In order to send a Text Message to the Site All Call Text ID, the source radio must have the "Site All Call Text Init" privilege enabled on its user record in the controller's user database.

4.10.20 Emergency Alert and Emergency Call in Connect Plus

Section 2 provides an introduction to Connect Plus emergency operation in the section entitled "Connect Plus Digital Emergency". Topics covered in that section include:

- Emergency features shared with other MOTOTRBO digital modes

- Emergency enhancements provided by Connect Plus

- Differences between Digital Emergency in Connect Plus and non-Connect Plus Modes.

This section expands on the information provided in Section 2 by elaborating on following topics:

- Sending an Emergency Alert in Connect Plus

- Making an Emergency Call in Connect Plus

- Emergency Calls on the SU's Multigroup ID

- Programmable Emergency Settings in MOTOTRBO Option Board Connect Plus CPS

- Programmable Emergency Settings in MOTOTRBO Connect Plus Network Manager

- Programming the repeater's Emergency Call Hang Time
- Emergency Handling Considerations
- Conducting Emergency Drills

4.10.20.1 Sending an Emergency Alert in Connect Plus

In Connect Plus, the radio's "Emergency Mode" is configurable per Connect Plus zone with MOTOTRBO CPS. When the Emergency Mode is configured as "Emergency Alert", a radio user initiates an Emergency Alert by pressing the "Emergency On" button configured for the unit with MOTOTRBO Connect Plus Option Board CPS.

If the button is pressed while the radio is idle and monitoring the Control Channel timeslot, the SU will immediately transmit its Emergency Alert on the Control Channel uplink. If the SU is involved in a call in progress when the radio user presses Emergency On, the SU leaves the trunk-to timeslot and returns to the Control Channel timeslot to transmit its Emergency Alert. If the SU is not currently registered to a site when the user presses Emergency On, the SU searches for a site. Upon detecting a qualified site, the SU transmits a Registration Request. Upon receiving its Registration Response from the XRC, the SU immediately and automatically transmits its Emergency Alert on the Control Channel uplink. Whenever the SU transmits an Emergency Alert, the Group ID it uses is determined by its "Revert Group" setting for its current Connect Plus zone. When "Emergency Alert" is the configured Emergency mode, the "Revert Group" setting must be configured for "Default Emergency Revert Group ID". This is discussed in greater detail in a subsequent section.

The SU will persistently send its Emergency Alert until it receives a response from the XRC controller. If multiple SUs are transmitting an Emergency Alert, each SU expects an individual response from the XRC, and the SU will continue to transmit the Emergency Alert until it receives one. The controller's response tells the SU whether it needs to send an Emergency Location Update at the end of the Emergency Alert session. The request for the Emergency Location Update is initiated by a 3rd Party LRRP application, and the application must send the request to the controller prior to the SU's emergency.

The emergency ergo for an Emergency Alert initiator is determined by the MOTOTRBO Connect Plus Option Board CPS "Emergency Initiation" settings. If the Emergency Type is set to "Regular", then the SU periodically transmits a Hi/Low tone from the time it sends its first Emergency Alert until it decodes a controller response. Upon decoding the controller's response, the SU sounds a positive indicator tone and displays, "Emergency Alert success". The radio then exits Emergency Alert mode. Emergency Alert signaling takes place entirely on the Control Channel timeslot. Emergency Alert is not followed by an Emergency Call. If the radio user presses PTT after the radio exits Emergency Alert mode, the radio will request a non-emergency call on the Contact Name that has been programmed for the currently selected Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio).

The emergency ergo for an Emergency Alert receiver is determined by the MOTOTRBO CPS Connect Plus Option Board CPS "Emergency Alert Receive" settings. These settings are explained in greater detail in a later section.

4.10.20.2 Making an Emergency Call in Connect Plus

In Connect Plus, a radio user initiates an Emergency Call by pressing the "Emergency On" button configured for the unit with MOTOTRBO Connect Plus Option Board CPS.

If the button is pressed while the radio is idle and monitoring the Control Channel timeslot, the SU will immediately transmit its Emergency Call Request on the Control Channel uplink. If the SU is involved in a call in progress when the radio user presses Emergency On, the SU leaves the trunk-to timeslot and returns to the Control Channel timeslot to transmit its Emergency Call Request. If the SU is not currently registered to a site when the user presses Emergency On, the SU searches for a site. Upon detecting a qualified site, the SU transmits a Registration Request. Upon receiving its Registration Response from the XRC, the SU immediately and automatically transmits its Emergency Call Request on the Control Channel uplink. Whenever the SU transmits an Emergency Call Request, the Group ID it uses is determined by its “Revert Group” setting for its current Connect Plus zone. This is described in greater detail in a later section.

The SU will persistently send its Emergency Call Request until it receives acknowledgement from the XRC controller. If multiple SUs are transmitting an Emergency Call Request, each SU expects an individual acknowledgement from the XRC, and the SU will continue to transmit the Emergency Call Request until it receives one. The controller’s acknowledgement message will either contain the assigned repeater and slot, or it will inform the SU that the call has been assigned to the Busy Queue. The controller’s acknowledgement also tells the SU whether it needs to send an Emergency Location Update at the end of the Emergency Call. The request for the Emergency Location Update is initiated by a 3rd Party LRRP application, and the application must send the request to the controller prior to the SU’s emergency.

If the call is assigned to the Busy Queue, it will be assigned the next available trunk-to timeslot. The only exception to this rule is when there are multiple Emergency Calls (for different Group IDs) in the Busy Queue. In that event, the Emergency Calls are assigned from the Busy Queue on a first-in, first-out basis. However, all Emergency Calls will be assigned prior to any non-emergency call.

The emergency ergo for an Emergency Call initiator is determined by the MOTOTRBO Connect Plus Option Board CPS “Emergency Initiation” settings. The emergency ergo for an Emergency Call receiver is determined by the MOTOTRBO CPS Connect Plus Option Board CPS “Emergency Receive” settings. These settings are explained in greater detail in a later section.

In most cases, there is just one initiator associated with an Emergency Call. However, it is possible that multiple radio users with the same Revert Group may press Emergency On during the same call (and using the same Group ID). In this case, each initiating SU will receive an individual acknowledgement from the XRC, but each controller response will assign the call to the same repeater and slot. (Other sites may also be carrying the same Emergency Call, but each site assigns its repeater and slot independently of other sites in the call). Any user participating in the Emergency Call on the Revert Group can transmit on the channel either by manual key-up or Hot Mic.

The emergency initiator is usually the first radio to transmit during the Emergency Call. If enabled for “Emergency Call with Voice to Follow”, the radio automatically transmits with microphone open for the duration of a programmable timer. After the initial transmission, the repeater uses the Emergency Call Hang Time. It is very important to program the same Emergency Call Hang Time in all Connect Plus repeaters and sites network-wide. During the Emergency Call Hang Time, any radio that has joined the call may transmit. During a typical emergency call there will be transmissions by one or more radio users that pressed the Emergency On button and transmissions by other radio users that did not press the Emergency On button. Receiving radios know whether or not the current voice transmission is coming from an emergency initiator. Radios that have been enabled for Emergency Call receive ergonomics will show the individual ID(s) of the emergency initiator(s) on their display, but they will not show the individual ID(s) of transmitting radios that are not “emergency initiators” (in other words, the radio user has not pressed Emergency On).

If the Emergency Call Hang Time expires with no more key-ups, the Emergency Call ends and all radios return to the Control Channel timeslot. Unlike other MOTOTRBO digital modes, this causes the initiating radio(s) to automatically exit emergency mode. If any emergency initiator feels that the call did not adequately address his/her emergency, then he/she should press Emergency On again to re-initiate the process.

4.10.20.3 Emergency Calls on the SU's Multigroup ID

Depending on how the radio is configured with MOTOTRBO Connect Plus Option Board CPS, it is possible that the SU may send the Emergency Call Request using its Multigroup ID. If so, it is important to understand two important differences between Emergency Calls on the Multigroup ID and non-emergency calls on the Multigroup:

- Each user record in the XRC provides a programmable call-initiation privilege for the Multigroup ID that can be enabled using the MOTOTRBO Connect Plus Network Manager. This programmable privilege applies to non-emergency calls only. It does not apply to Emergency Calls. When the SU sends an Emergency Call Request using its Multigroup ID, the XRC only checks whether the unit has the programmable Emergency Initiation privilege (discussed in a later section). If so, the Emergency Call is allowed, regardless of whether or not the unit has non-emergency Multigroup initiation privileges.

- During non-emergency Multigroup calls, only the initiating SU allows PTT during Group Call Hang Time. During emergency calls using the Multigroup ID, any Connect Plus SU programmed with a matching Multigroup ID is allowed to talk-back during the Emergency Call Hang Time.

4.10.20.4 Programmable Emergency Settings in Option Board CPS

MOTOTRBO Connect Plus Option Board CPS provides multiple programmable settings that affect Emergency operation in the Connect Plus SU. Some of these settings affect all Connect Plus zones. The remaining settings can be configured per Connect Plus zone.

Emergency Settings that affect all Connect Plus zones

Connect Plus provides the same programmable options for the Emergency Button as other digital modes. On the portable radio, only the orange button can be configured for emergency. On the mobile radio, any of the configurable buttons can be set for emergency. "Emergency On" can be configured as either a short press or a long press. "Emergency Off" will automatically be the other selection for the same button. For example, if "Emergency On" is configured as a short press of the orange button, "Emergency Off" will automatically be configured as a long-press of the same button.

Connect Plus provides a configurable timer called "Emergency Short Press Duration". When "Emergency On" has been configured as a short press, this timer determines how long the button must be held before the Connect Plus SU transmits an Emergency Alert or Emergency Call Request. The purpose of this timer is to prevent short, accidental presses from starting an Emergency Alert or Emergency Call.

MOTOTRBO Connect Plus Option Board CPS provides a programmable option on the **Networks** screen to define a "Default Emergency Revert Group". If used for Emergency Call, any Group contact in any Connect Plus zone (except Site All Call) can be set as the "Default Emergency Revert Group". If any Connect Plus zone is configured for "Emergency Alert" as the Emergency Mode, then the Default Emergency Revert Group ID must not be set for "Multigroup". It must be configured for a regular Group Contact that is not used for any type of voice call. In other words, the Group Contact selected as the "Default Emergency Revert Group ID" must not be assigned to any Channel Selector Knob or Channel Rocker position in any Connect Plus radio zone with the same Network ID. The intent of this rule is to prevent the ID from already being in use for a voice call when the radio user presses "Emergency On" to initiate an Emergency Alert. If this were occur due to mis-configuration, the radios involved in the voice call would not be aware of the Emergency Alert.

If the SU is configured with a Default Emergency Revert Group, the same Group ID must be configured as the Default Emergency Revert Group on the SU's user record in the XRC (using MOTOTRBO Connect Plus Network Manager). If there is a mismatch between Default Emergency Revert Group programming in the Connect Plus SU and the XRC controller, the Emergency Call may not work as expected. This is one reason why it is critical to

run an Emergency drill prior to using the feature in an actual emergency. The Emergency drill will help catch any configuration issues prior to a real emergency.

Emergency Settings per Connect Plus zone

The configurable settings per Connect Plus zone fall into two categories; settings that affect Emergency Alert or Emergency Call initiation and settings that affect how the SU receives an Emergency Alert or Emergency Call.

Emergency Initiation Settings

- **Emergency Type**: MOTOTRBO Connect Plus Option Board CPS provides four configurable options for Emergency Type; Disabled, Regular Emergency, Silent Emergency, and Silent Emergency with voice. The Silent Emergency options provide a means to suppress all indications of the emergency status on the initiating radio. This feature is valuable in situations where an indication of an emergency state is not desirable. There are two programmable variations of Silent Emergency; “Silent” and “Silent with voice”. The operation for “Silent” and “Silent with voice” depends on whether the Emergency Mode is configured for Emergency Call (including Emergency Call w/voice to follow) or Emergency Alert. For more information, see section Emergency Handling Considerations.

- **Emergency Mode**: MOTOTRBO Connect Plus CPS provides three programmable options for Emergency Mode; Emergency Alert, Emergency Call and Emergency Call with voice to follow.

  If the Emergency Mode is set for “Emergency Alert”, then the radio will indicate its Emergency condition through Control Channel signaling only. Emergency Alert is not followed by an Emergency voice call. Because Emergency Alert signaling occurs entirely on the Control Channel timeslot, an Emergency Alert never has to wait in the Busy Queue.

  When Emergency Alert is not configured as the Emergency Mode, then pressing “Emergency On” requests the radio to start to Emergency Call. Whether the radio is configured for “Emergency Call” or “Emergency Call with voice to follow” as the Emergency Mode determines how the SU makes it first transmission after synching with the trunk-to timeslot. If “Emergency Call with voice to follow” is enabled, the SU automatically transmits with microphone open for the duration of the “Hot Mic Duration” timer. When “Emergency Call” is enabled, the SU will only make a brief, automatic transmission upon synching with the voice channel. The purpose of the transmission is to start the Emergency Call on the trunk-to timeslot.

- **Revert Group**: Each Connect Plus zone provides two configurable options for Revert Group; “Selected Registration Group ID” or “Default Emergency Revert Group ID”. Because this is one of the most important decisions when configuring Connect Plus emergency operation, there is an in-depth discussion on these options in the later section, “Emergency Handling Considerations”. When the Emergency Mode is set to “Emergency Alert”, then the “Revert Group” field must be set to “Default Emergency Revert Group ID”.

- **Emergency Attempts**: MOTOTRBO Connect Plus Option Board CPS provides a configurable setting called “Emergency Attempts”. If the Connect Plus SU sends all Emergency Attempts and gets no response from the XRC controller, it will Search for a different site. Upon locating a Connect Plus site (which might be the same site the SU tried previously – especially in a single-site network or a multisite network without overlapping coverage), the Connect Plus SU starts over on its Emergency Attempts.

- **Hot Mic Duration**: When “Emergency Call with Voice to Follow” is selected as the Emergency Mode, this configurable timer determines how long the SU automatically transmits with microphone open after aligning with the assigned trunk-to timeslot.

Emergency Call Receive Settings

For portable and mobile radios equipped with a display, MOTOTRBO Connect Plus Option Board CPS has two programmable options for Emergency Call Receive settings; “Emergency Alert Tone” and “Emergency Call Indication”.

- **Emergency Alert Tone**: When “Emergency Alert Tone” is enabled, the Connect Plus SU will emit a periodic and distinctive tone at the beginning of the Emergency Call. The tone will persist until the radio user acknowledges by pressing any button. Even after the radio user acknowledges the tone, emergency display ergo will continue (even after the call ends) until the radio user clears the ergo. The procedure for clearing Emergency display ergo varies by radio model. For more information, see the Connect Plus subscriber radio user guide for the specific model of interest.

- **Emergency Call Indication**: When “Emergency Call indication” is enabled, the SU toggles the radio display to provide information about the Emergency Group ID and the SUID that started the Emergency Call (or the last SU to transmit emergency voice during the call). This display ergo automatically stops when the Emergency Call ends (unless “Emergency Alert Tone” has also been enabled). When neither option is enabled (as will always be the case for the non-display portable or numeric display mobile), the receiving SU provides the same ergo as it provides for a non-emergency Group Call.

- **Ignore EM Revert Call RX (Ignore Emergency Revert Call Receive)**: When this feature is enabled, the radio user can initiate an Emergency Call on a specific Default Emergency Revert Group ID, but cannot listen in on an Emergency Call that was initiated by a different radio on the same Default Emergency Group ID. Radios that are configured to “Ignore EM Revert Call RX” will not provide any indication of the ongoing Emergency Call, unmute to voice, or allow transmission during the call (unless they are an Emergency Call initiator).

Emergency Alert Receive Settings

For portable and mobile radios equipped with a display, MOTOTRBO Connect Plus Option Board CPS currently has one programmable option for Emergency Alert Receive settings; “Alert Indication”.

- **Alert Indication**: When “Alert Indication” is enabled, and when the Connect Plus SU decodes an Emergency Alert containing a Group ID that matches its Default Emergency Revert Group ID, the Connect Plus SU will emit a periodic and distinctive tone. The tone will persist until the radio user acknowledges by pressing any button. Even after the radio user acknowledges the tone, emergency display ergo will continue until the radio user clears the ergo. The procedure for clearing Emergency display ergo varies by radio model. For more information, see the Connect Plus subscriber radio user guide for the specific model of interest. If “Alert Indication” is not enabled (as will always be the case for the non-display portable or numeric display mobile), the radio provides no ergonomic indication whatsoever upon decoding an Emergency Alert.

4.10.20.5 Programmable Emergency Settings in XRC Controller

The XRC controller has three programmable settings that affect Emergency Alert and/or Emergency Calls. These settings are configured with the MOTOTRBO Connect Plus Network Manager.

Emergency Call Hang Time: The Emergency Call Hang Time value that is programmed with MOTOTRBO CPS will be overwritten by the XRC when it establishes its link with the repeater. In doing so, the XRC uses the Emergency Call Hang Time value that has been programmed with the MOTOTRBO Connect Plus Network Manager. The programmable range provided by the Network Manager is considerably higher than the programmable range provided by MOTOTRBO CPS. The repeater will use the Network Manager-configured

value as long as it maintains its connection to the XRC. See section “Programming the Repeater’s Emergency Call Hang Time” for important information on configuring this timer.

Each user record in the XRC has two very important settings on the “User Details” screen.

Emergency Init (checkbox): Enable this checkbox to allow this SU to send an Emergency Alert or Emergency Call Request. Whether the SU sends an Emergency Alert or an Emergency Alert is determined by how the SU is programmed with Connect Plus CPS. Disable (uncheck) the box if the SU should not be allowed to request an Emergency Alert or Emergency Call. In this event, the Emergency Alert or Emergency Call Request will be denied. The controller provides the ability to deny emergency privileges to some SUs to prevent non-critical, low priority users from using Emergency to circumvent their low priority status.

Default Emergency Revert Group ID: This setting is used to tell the XRC whether the SU has a Default Emergency Revert Group, and – if so – which Group is used. In order to correctly configure Default Emergency Revert Group, it is necessary to know how the subscriber unit has been (or will be) programmed with Connect Plus CPS.

Enable the “None” bullet if the SU will not be sending Emergency Call or Emergency Alert Requests, or if the SU will only be sending Emergency Call Requests using its selected Registration Talk Group ID.

Enable the “Use Multigroup ID” bullet if this SU will be using its Multigroup ID as its Default Emergency Revert Group ID. Do not select this bullet if the SU is configured for “Emergency Alert” as its Emergency Mode with Connect Plus CPS.

If the SU will be using some other Group as its Default Emergency Revert Group, enable the “Use” bullet and enter the Group number to be used in the programmable field. There must be a matching Group record for this ID in the XRC. If the SU is configured with Connect Plus CPS to use “Emergency Alert” as its Emergency Mode, it will send the Emergency Alert on its Default Emergency Revert Group ID. In this case, the Group ID entered into this field should be dedicated to Emergency Alert signaling. It should not be used for any type of voice communications. If this were to occur, the voice communications could prevent radios from receiving the Emergency Alert.

Important: If a Default Emergency Revert Group is used, then the same Default Emergency Revert Group ID must be configured in both the SU (using MOTOTRBO Connect Plus Option Board CPS) and in the XRC user record (using MOTOTRBO Connect Plus Network Manager). It is critical for this information to match in both places. A mis-match of Default Emergency Revert Group information is a critical programming error that will cause undesired operation.

4.10.20.6 Programming the Repeater's Emergency Call Hang Time

Emergency Hang Time: The Emergency Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Emergency Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager.

Many systems set the Emergency Call Hang Time to a higher value than the Group Call Hang Time and the Private Call Hang Time. This provides increased time for talk-back during the Emergency Call and helps prevent the assigned Emergency timeslot from being released too soon. The Network Manager allows the Emergency Call Hang Time to be configured up to a maximum of 600 seconds. For whatever value is configured for the Emergency Call Hang Time, the repeater will stay on the air (with the Hang Time) for the full configured duration after the last key-up in the call. Prior to setting the Emergency Call Hang Time to a long value, the Radio System Administrator should carefully consider how a long Hang Time can affect operation:

1. Radios that were currently in the Emergency Call will not be able to easily leave the call (if at all) until the Emergency Call Hang Time expires. This is especially true for the Emergency initiator, but it is also true for radios that were merely receiving the Emergency. Even if the user changes the Selected Talk Group, the radio will be immediately drawn back into the call (after re-registering with the site) if the call is occurring on the user's Emergency Revert Group ID, Multigroup ID, or a Group ID that is an active member of a currently enabled scan list.

2. Until the Emergency Call Hang Time expires, late joiners will continue to join the call, even if no one is currently speaking.

3. If any radio user presses PTT before the Emergency Call Hang Time expires, it will reset the Emergency Call Hang Time to its full value at the end of the transmission, thereby prolonging the operation described in #1 and #2.

4.10.20.7 Emergency Handling Considerations

Configuring a communication system (like MOTOTRBO Connect Plus) to handle emergency situations requires some up front design. In emergency situations, it is ideal that when a user initiates an emergency, he is immediately routed to someone who can handle his emergency situation. In order for this occur, several things must be in place:

- The Connect Plus SU and the XRC should already be configured with the Emergency Settings desired by the customer. The configuration is impacted by questions such as the following:
  - Which Emergency Mode is desired for this SU, Emergency Alert mode or one of the Emergency Call modes?
  - Who is allowed to initiate an Emergency Alert or Emergency Call?
  - What should the ergo look like for the initiating radio?
  - Who is allowed to receive an Emergency Alert or Emergency Call?
  - Who should the ergo look like for the receiving radio?
  - What ID should be used for the Emergency Alert or Emergency Call?
  - How long should the Emergency Hang Time be between Emergency Call key-ups?

- The radio user should be trained in (a) what circumstances constitute an emergency, (b) how to initiate the Emergency Alert or Emergency Call on the SU (c) what to do when initiating and/or receiving an Emergency Alert or Emergency Call and (d) the organization's emergency protocol & procedures, which should address the following:
  - Who is responsible for responding to the emergency?
  - Who is responsible for handling the emergency communications?
  - Who is allowed (or not allowed) to talk during an Emergency Call?
  - Who decides when the emergency is over?

The considerations listed above apply both to Connect Plus and to non-Connect Plus digital modes. However, there are some considerations that apply to other digital modes that do not apply to Connect Plus. These include the following:

- In Connect Plus, it is not necessary to decide in advance which site, repeater and timeslot to use for Emergency Call. The Emergency Call Request is sent to the registered site, and the call is assigned to a repeater and slot by the XRC controller.
- In other MOTOTRBO digital modes, it is very important to understand the interactions between the Selected Channel, the Emergency Revert Channel, and the Data Revert Channel. In Connect Plus, the Control Channel timeslot is the most important path between the system and the SU. The controller picks which repeater and slot to use for Emergency Call and/or Emergency Location Update, and informs SUs via messaging on the Control Channel timeslot.
- In Connect Plus, it is not necessary to decide which supervisor radios should send over-the-air acknowledgement to the Emergency. In Connect Plus, the XRC controller individually responds to each Emergency Alert or Emergency Call Request. Over-the-air acknowledgement by a subscriber unit is neither necessary nor currently supported in Connect Plus. Because of this difference, the roles of "Monitoring Supervisor" and "Acknowledging Supervisor", which are usually identified as two separate roles in other MOTOTRBO Digital Modes (see MOTOTRBO System Planner for more information on user roles), can be fulfilled by a single individual in Connect Plus.
- In Connect Plus, it is not necessary to assign a different individual to monitor for (and respond to) emergency at each network site. This is because the Connect Plus infrastructure will automatically route the Emergency Alert or Emergency Call to each and every site where the Group ID used for the emergency is currently registered.

Selecting the Emergency Mode

Perhaps the most important decision when determining a radio's Emergency Initiation settings is deciding whether an "Emergency On" button press should initiate an Emergency Alert or one of the two Emergency Call settings (Emergency Call or Emergency Call with voice to follow). The Emergency Mode setting also determines what type of emergency is automatically initiated by a Man Down alarm on a Connect Plus portable radio. (Man Down is a purchasable Connect Plus feature).

Although Connect Plus CPS configuration makes it theoretically possible to select "Emergency Alert" as the Emergency Mode in some connect Plus zones and one of the Emergency Call options as the Emergency Mode in other Connect Plus zones, this programming strategy is not recommended. Instead, it is strongly recommended to decide which Emergency Mode option will be utilized, and to configure this as the Emergency Mode in all Connect Plus zones. Having just one Emergency Mode radio-wide reduces confusion for both the Emergency initiator and the Emergency receiver. It also reduces the complexity of Connect Plus CPS programming. If the customer requires some zones to be configured for Emergency Alert and other zones to be configured for

Emergency Call or Emergency Call w/voice to follow, the Revert Group configuration must conform to the following rules:

1. In the Emergency Alert zone(s), Revert Group must be set to “Default Emergency Revert Group ID” only.

2. In the Emergency Call (or Emergency Call with voice to follow) zone(s), Revert Group must be set to “Selected Registration Talk Group ID” only.

The following bullets summarize some pertinent information for determining the SU’s Emergency Mode:

Emergency Alert Mode

- Emergency Alert signaling occurs entirely on the Control Channel timeslot. Because of this, Emergency Alert never has to wait in the Busy Queue.

- Emergency Alert provides fewer options (than Emergency Call) for which Group ID is used for the Emergency. The Emergency Alert must be sent on the SU’s Default Emergency Revert Group ID as configured with Connect Plus CPS. Also, the ID used for the Emergency Alert must not be used for any voice call. This means that the Group Contact used for Emergency Alert must not be assigned to any Channel Selector Knob position or any Channel Rocker position in any Connect Plus radio zone with the same Network ID.

- With Emergency Alert, a radio will not provide any indication of having decoded an Emergency Alert unless it has been enabled for “Alert Indication”. Even then, the radio only provides ergonomic indications or receiving an Emergency Alert when it is sent on an ID that matches the SU’s Default Emergency Revert Group ID.

- Because an Emergency Alert is not followed by an Emergency Call, it provides a range of options as to how to respond to the Emergency. Some possible examples include the following:

  - Supervisor radio or console operator can make a Private Call to the emergency initiator.

  - Supervisor radio or console operator can perform a Remote Monitor of the emergency initiator.

  - Conduct follow-up communications via a non-Emergency Group Call, utilizing a special Group ID allocated for this purpose. This approach would require the user to make a Group Change on his/her radio after sending the Emergency Alert. Do not use the Emergency Revert Group ID for voice communications. If this were to occur, it could prevent radios from receiving Emergency Alerts.

- Radios involved in calls-in-progress on trunk-to timeslots at the time the Emergency Alert is initiated will not be aware of the Emergency Alert unless the call-in-progress ends (through normal means) and the radio returns to the Control Channel timeslot while the controller is still repeating the Emergency Alert message. The controller repeats the Emergency Alert message a total of five times (even if the source radio displays “Emergency Alert Success” the first time the controller repeats the Emergency Alert CSBK). The minimum interval between each repeat of the Emergency Alert message is determined by “CSBK Retry Interval” as configured with the Network Manager. At the default setting, the minimum interval between each repeated Emergency Alert message is approximately two seconds, but the interval can be longer if the Control Channel has many call messages to send. This means that the entire duration of Emergency Alert signaling for a single Emergency Alert event is typically between eight and ten seconds, but can be somewhat longer depending on Control Channel activity.

- Connect Plus CPS provides two configurable Silent Emergency Types (“Silent” and “Silent with voice), which can be used to suppress the audible and visual emergency indications on the initiating radio. How long the silent ergo persists, and whether the silent ergo is cancelled manually or automatically, depends

on the combination of settings for Emergency Type and Emergency Mode. For Emergency Alert and Emergency Call, there is a difference in the operation of “Silent” and “Silent with voice” Emergency Types.

- When Emergency Mode is configured for Emergency Alert: If the source radio is configured for “Silent” Emergency Type, the “silent” ergo continues to persist, even after the Emergency Alert session is over. The silent ergo must be cancelled by the radio user. The radio user can cancel the “silent” ergo by pressing PTT or “Emergency Off”. If the source radio is configured for “Silent with voice” Emergency Type, the Connect Plus radio automatically cancels the silent ergo when it sees its Emergency Alert repeated on the Control Channel downlink. It will then receive and/or initiate calls in the normal manner.

- When Emergency Mode is configured for Emergency Call or Emergency Call w/voice to follow: If configured for “Silent” Emergency Type, the radio mutes the speaker and does not provide any audio or visual indication that it has requested an Emergency Call. If configured for “Silent with voice”, the radio does not provide any audio or visual indication that it has requested an Emergency Call, but it will unmute to received voice transmissions during the Emergency Call. Regardless of whether the Emergency Type is “Silent” or “Silent with voice”, the silent ergo does not persist after the Emergency Call ends. After the Emergency Call ends, the radio automatically returns to regular ergo. During the Emergency Call, the radio user can cancel the “silent” ergo can by pressing PTT.

Emergency Call Mode (Emergency Call and Emergency Call with voice to follow)

- Emergency Call signaling occurs partially on the Control Channel timeslot and partially on the voice timeslot assigned for the Emergency Call. If a voice resource is not available, the Emergency Call will have to wait in the Busy Queue for a resource to become available. Because Emergency Calls immediately go to the top of the Busy Queue, it will receive the next available timeslot (unless there are other Emergency Calls already in the Busy Queue.)

- If a radio is enabled for Emergency Call receive ergo, it will provide Emergency Call ergo for a wider-range of Group IDs than Emergency Alert. The Connect Plus radio provides Emergency Call receive ergo upon decoding an Emergency Call on any of the following IDs:

  - Selected Registration Group ID
  - Default Emergency Revert Group ID (if one is configured through Connect Plus CPS programming)
  - Multigroup ID
  - Any currently enabled scan list member

- If Emergency situations involve voice communications, there are several significant advantages to providing voice communications via Emergency Call rather than Emergency Alert followed by a non-emergency voice call. These advantages include:

  - Preferential treatment for the call in the Busy Queue (Emergency Call is top of queue)

  - Emergency Call has a longer configurable call hang time. This means that it is less likely that the assigned timeslot will be accidentally lost due to pause between radio transmissions.

  - If a radio is involved in another call (or not registered to the site) when the Emergency Call starts, it will join the call in-progress if the Emergency Call is still underway when the previous call ends (or after the radio registers to the site). Even though the radio is a late joiner, it will provide Emergency receive indications (if so configured) upon joining the call.

- An Emergency Call usually lasts longer than an Emergency Alert session. This is because the Emergency Call typically consists of one or more radio key-ups, plus the Emergency Call Hang Time following each key-up. The longer duration provides a larger “window” for late joiners. Because of this, receiving radios are less likely to miss an Emergency Call than an Emergency Alert.

Identify Emergency Initiators

One of the first steps is to identify the radio users that may find it necessary to request an Emergency Call. The following questions are pertinent to Emergency Initiators:

- Who is allowed to initiate an Emergency Alert or Emergency Call? Emergency initiators require the “Emergency Init” privilege on the SU’s user record in the XRC controller (using MOTOTRBO Connect Plus Network Manager). The “Emergency Init” privilege allows the radio user to start either an Emergency Alert or Emergency Call, depending on how the radio is programmed with Connect Plus CPS.

- What should the ergo look like for the initiating radio? MOTOTRBO Connect Plus Option Board CPS provides configurable options to determine whether the radio sends a “Regular” or “Silent” emergency. It also provides an option to determine whether or not the radio should do an automatic “hot mic” key-up at the beginning of an emergency call, and – if so – for how long.

Identify Emergency Receivers and/or Responders

Another important step is to identify which radios should be able to receive an Emergency Alert and/or Emergency Call, and which individuals are responsible for responding to the emergency.

An “Emergency Receiver” is a person that is allowed to receive an emergency call, but doesn’t necessarily have the responsibility for responding to the crisis. The primary role of the “Emergency Receiver” is to help make sure that the “Emergency Responder” is aware of the emergency, and to render assistance when and if requested.

The “Emergency Responder” is an Emergency Receiver with responsibilities above and beyond those of other receivers. The “Emergency Responder” takes an active role in coordinating the emergency response and resolving the crisis.

The following questions are pertinent to Emergency Receivers and Responders

- Who is allowed to receive an Emergency Call? These radio users should be equipped with display capable radios (since the non-display portable and numeric display mobile provide no special ergo while receiving an Emergency Alert and/or Emergency Call). Additionally, these display radios should be configured with the Group ID(s) that will be used during the Emergency Alert and/or Emergency Call(s).

What should the ergo look like for the receiving radio? A display-equipped radio can be configured with Connect Plus CPS to provide Emergency Receive indication upon decoding an Emergency Alert only, upon receiving an Emergency Call only, upon receiving either an Emergency Alert or Emergency Call, or to never provide Emergency Receive indications. For Emergency Alert Receive ergo, there is currently just one configurable option (to provide Emergency Alert receive indication or not). When Emergency Alert Receive Indication is enabled, and when a radio decodes an Emergency Alert that matches its Default Emergency Revert Group, the radio provides an Emergency Alert tone and a persistent Emergency display showing the alias or ID of the Emergency initiator. The radio user clears the tone and the display through two different actions. For Emergency Call, there are three programmable options for Emergency Call Receive ergo; “Emergency Alert Tone”, “Emergency Call Indication”, and “Ignore EM Revert Call RX” (Ignore Emergency Revert Call Receive).

- Emergency Alert Tone is considered to be a more aggressive form of emergency receive ergo that is especially appropriate for Emergency Responders. The recurring tone and Emergency display will each

persist until manually cleared by the radio user. Clearing the tone and clearing the Emergency display are separate operations.

- Emergency Call Indication is considered to be a less aggressive form of emergency receive ergo. It involves the display only (no tone) and does not have to be manually cleared. The Emergency display automatically returns to normal when the Emergency Call ends. This option is appropriate for Emergency Receivers.

- When “Ignore EM Revert Call RX” is enabled, the radio user can initiate an Emergency Call on a specific Default Emergency Revert Group ID, but cannot listen in on an Emergency Call that was initiated by a different radio on the same Default Emergency Group ID. Radios that are configured to “Ignore EM Revert Call RX (Ignore Emergency Revert Call Receive)” will not provide any indication of the ongoing Emergency Call, unmute to voice, or allow transmission during the call (unless they are an Emergency Call initiator). The radios of Emergency Receivers and Responders should not be enabled for this option.

It should be noted that both Emergency Alert Tone and Emergency Call Indication can be enabled in the same radio. Another option is to enable neither receive option. In this case, the radio receives the Emergency Call just like other Group Calls.

Emergency Receive-Only Configuration

In most Emergency management implementations, radios that are allowed to receive Emergencies (and to provide Emergency Receive indications to the radio user) are also allowed to initiate Emergencies. The special case where the SU is allowed to receive an Emergency, but not to initiate one, merits some discussion.

In Connect Plus CPS the Emergency Initiation Settings and the Emergency Receive settings are configured separately. These settings are located on the Zone Emergency Screen. To prevent the SU from sending an Emergency when selected to this zone, set the Emergency Type to “Disabled”. (Emergency Type is one of the Emergency Initiation settings). The Emergency Call Receive settings and the Emergency Alert Receive Settings can be enabled independently of the Emergency Initiation settings. These settings determine whether the SU shall provide Emergency Receive ergo upon decoding an Emergency Call on a Group ID of interest or an Emergency Alert on the SU’s Default Emergency Revert Group ID.

On the Connect Plus CPS Buttons screen, assign a button for Emergency On/Emergency Off – even if the SU is not configured to initiate an Emergency Call in any zone. This is because the Emergency Off button is used in some models as part of the special button sequence to clear persistent Emergency Receive Ergo. This button assignment will not cause the SU to initiate an Emergency if the SU is operating in a zone where the Emergency Type is configured for “Disabled”. If the user attempts to press “Emergency On”, the display shows, “Emergency Not Available”, and the SU will not transmit an Emergency request to the site controller.

On the Connect Plus CPS **Networks** screen, it will be necessary to assign a Group Contact to the Default Emergency Revert Group ID field if the initiating radio uses the Default Emergency Revert Group ID to send its Emergency. For Emergency Call this depends on whether the initiating radio is configured to start the Emergency Call on “Default Emergency Revert Group ID” or “Selected Group ID”. For Emergency Alert, the initiating radio can only use the Default Emergency Revert Group to send its Emergency Alert.

If Default Emergency Revert Group is part of the Emergency implementation, there is an additional configuration step that needs to be taken in the MOTOTRBO Connect Plus Network Manager. This is required whether the SU can initiate Emergencies, or only receive them. Use the Network Manager to connect to the XRC Controller and open the user record for the radio that is being configured. Set the Default Emergency Revert Group to match the Default Emergency Revert Group configured into the radio with Connect Plus CPS. The controller will automatically register this Group to any network site visited by this SU. This provides assurance that the Emergency Call (or Emergency Alert) will be networked to the SU’s registered site.

Radio Users with Multiple Roles

It should be noted that a single individual may be both an Emergency Initiator and an Emergency Receiver, and it is also possible for a single person to be in all three categories (Emergency Initiator, Emergency Receiver, and Emergency Responder.) When a single individual has multiple roles, this should be considered with programming the SU with MOTOTRBO Connect Plus Option Board CPS.

Selecting which Group ID is used for the Emergency Call or Emergency Alert

One of the most important decisions when configuring the Emergency Options for a Connect Plus radio is which Group ID to use for the Emergency Alert or Emergency Call. This is determined by the “Revert Group” setting. MOTOTRBO Connect Plus Option Board CPS provides two programmable options per Connect Plus zone; “Selected Registration Talk Group ID” or “Default Emergency Revert Group”.

If Emergency Alert is the configured Emergency Mode, then select “Default Emergency Revert Group” as the Revert Group setting. The specific Group contact that will be used as the Default Emergency Revert Group is configured on the Networks screen. If Emergency Alert is configured as the Emergency Mode option for any zone, do not use the Multigroup ID as the Default Emergency Revert Group ID. Configure the Default Emergency Revert Group for a Group contact that is not used for voice calls. This Group contact must not be assigned to Channel Selector Knob (or Channel Rocker) position in any radio. The Group ID that is configured as the Default Emergency Revert Group ID with Connect Plus CPS must also be configured as the Default Emergency Revert Group on the SU’s user record in the XRC controller (using the Network Manager).

If the radio is configured only for “Emergency Call” or “Emergency Call w/voice to follow” as the Emergency Mode, then “Selected Registration Talk Group ID” and “Default Emergency Revert Group” are both allowable Revert Group options. If “Selected Registration Talk Group ID” is chosen as the Revert Group, the Emergency Group ID is determined by the currently selected position on the Channel Selector Knob (portable) or Channel Rocker Knob (mobile). When the radio user presses “Emergency On”, the SU will send the Emergency Call Request using the Registration Talk Group ID as configured for that position with MOTOTRBO Option Board Connect Plus CPS. In most cases, this will be the same as the selected Group Contact name. However, when the selected Contact Name is a Private Call ID or Site All Call ID, the Group ID used for the emergency call is configurable by selecting any Group from the Zone Contact list (except Site All Call) as the Registration Group ID.

If “Default Emergency Revert Group” is selected as the Revert Group, the Emergency Call Request is sent using the “Default Emergency Revert Group” programmed onto the Networks screen. There is just one “Default Emergency Revert Group” per SU, and the Group number programmed into this field must match the Default Emergency Revert Group programmed in the XRC user record for this SU (using MOTOTRBO Connect Plus Network Manager).

There are several factors to consider when deciding which programmable option to use for the Emergency Call Revert Group.

Default Emergency Revert Group offers several attractive advantages. It allows the Emergency Call to always be sent on one specific Group ID, regardless of which position is currently selected on the Channel Rocker Knob (portable) or Channel Rocker (mobile). This strategy is sometimes referred to as a “centralized” approach for Emergency handling.

Because the Default Emergency Revert Group is programmed into the controller, the XRC automatically registers the SU to this group, no matter where it roams in the Connect Plus network. In effect, this can increase the number of Groups that a single SU carries network-wide from two to three (by adding the Default Emergency Revert Group to the SU’s currently Selected Registration Group ID and the SU’s Multigroup ID.) The SU automatically scans for Emergency Calls on its Default Registration Group ID anytime that it is idle no matter it is located in the network. On the plus side, this makes it likely that the SU will hear the Emergency Call, no matter which site the call is started at. A possible disadvantage is that it will be quite difficult for a receiving SU to “escape” from an Emergency Call in-progress in order to conduct voice communications on a different call (a different Group ID or a Private Call). Even if the radio user changes his/her radio to a different position on the

Channel Selector Knob(portable) or Channel Rocker (mobile), the radio will likely scan right back into the Emergency Call before the radio user can initiate the new call.
Another advantage of Default Emergency Revert Group is that many radios can be programmed to initiate an Emergency Call using this ID, but – if desired – a smaller set of radios can be programmed to decode (and un-mute to) Emergency Calls using the same ID. Radios that should not respond to the Emergency Call should be configured with “Ignore EM Revert Call RX” (Ignore Emergency Revert Call Receive). When this option is enabled with CP CPS, the radio user can initiate an Emergency Call on a specific Default Emergency Revert Group ID, but the radio will not provide Emergency ergo, un-mute, or allow voice transmission for an Emergency Call initiated by a different radio on the same Group ID. If any radio is configured to “Ignore EM Revert Call RX” (Ignore Emergency Revert Call Receive), then the Default Emergency Revert Group ID of that radio should not be assigned to a channel selector position in any fleet radio as this can cause undesirable operation for this feature.

Radios that are not configured to “Ignore EM Revert Call RX” (and that have been enabled for other Emergency Receive settings) will provide Emergency ergo upon decoding an Emergency Call on their Default Emergency Revert Group ID. They will also un-mute to voice and will allow voice transmission during the call.

It is recommended that the Default Emergency Group ID should be used for Emergency Calls or Emergency Alert only. It should not be used for non-emergency communications as this can cause result in non-optimal performance for several emergency-related features. To prevent the Default Emergency Group ID from being used for non-Emergency voice calls, do not assign it to a channel selector position for any fleet radio.

As a general rule, the “Selected Registration Talk Group ID” option would make it easier for *Emergency Receivers and Responders* to “escape” from an Emergency Call (by selecting a different Registration Talk Group). This would allow the SU to more easily conduct voice communications on a Private Call or a different Talk Group during an emergency call in-progress. The exception to this statement is if the SU’s Multigroup ID happened to be the currently selected Registration Talk Group ID. If the Emergency Call is sent on the Multigroup ID, the receiving SU will likely keep scanning back into the Emergency Call – even if the user selects a different Registration Talk Group ID. Another advantage of the “Selected Registration Talk Group” option is that it causes the radio to request the Emergency Call on the SU’s normal communications group. This is sometimes referred to as a “tactical” approach for emergency handling, and may be advantageous for some smaller organizations. A potential drawback to this option is the fact that the SU’s Emergency Group can change, depending on the currently selected Channel Selector Knob or Channel Rocker position. Because of this, a significant listener (such as a supervisor radio) can miss the Emergency Call if selected to a different position.

Although MOTOTRBO Connect Plus Option Board CPS makes it possible to choose “Registration Talk Group ID” as the Emergency Call Revert Group in one Connect Plus zone and “Default Emergency Revert Group” as the Emergency Call Revert Group in a different Connect Plus zone, this strategy is generally not recommended. Other radio users and the XRC controller do not know which Connect Plus zone is currently selected in a specific SU. Because of this (and also for the sake of consistency), it usually makes more sense to choose just one Revert Group strategy, and to utilize that strategy across all Connect Plus zones.

4.10.20.8 Conducting Emergency Drills

Once an emergency plan has been formulated, and it has been configured into the various components of the Connect Plus radio system, the next step is to conduct a well-conceived emergency drill prior to the first occurrence of an actual emergency.

The Emergency Drill provides the following benefits:

- It helps identify configuration issues that can prevent the Emergency Alert or Emergency Call from operating as intended. It is very important to detect and correct any such issues prior to the first real emergency. If the XRC detects certain configuration errors when a radio sends a request for Emergency Alert or Emergency Call, the controller creates an Event Log entry and raises a Controller Alert. Both the

Event Log entry and the Controller Alert are called, “Emergency Configuration Error”. These are raised at the site where the radio transmits the Emergency Alert or Emergency Call. To correct the Emergency Configuration Error it may be necessary to edit one or more user records (using the Network Manager), and/or to edit the Option Board codeplug (using Connect Plus CPS). If the underlying problem is not corrected, the Emergency Configuration Error will be raised again the next time the radio attempts to send an Emergency Call or Emergency Alert. It is possible that the controller may detect more one than one configuration error for a single Emergency Call or Emergency Alert request. If so, this can result in multiple Event Log entries with the same timestamp. See the Event Log entry for the following details: (a) Date & Time, (b) the Source Radio ID, (c) the Destination Group ID, (d) the error reason. The following configuration errors will cause the Event Log message to be raised:
  - Source ID not is not enabled for Emergency Initiation privilege
  - Either Source or Destination ID is “disabled” (or does not exist) in the user registry
  - Destination Group ID is not registered to site
  - Destination Group ID for Emergency Alert is not the same as the Default Emergency Revert Group ID on user record for the Source SU.

- It helps radio users become familiar with the emergency operation of the Connect Plus SU and the Connect Plus infrastructure. Otherwise, the radio may user may never experience this emergency operation and ergo prior to the first actual emergency.

- It helps radio users practice the organization’s protocol and procedures for initiating and responding to an emergency situation.

- It helps identify the “weak links” in the organization’s emergency plan. (Those things that require more thought, additional practice, or both).

If is important to note that an Emergency Drill should not just be a one-time event. Emergency drills should be scheduled at regular intervals in order so that everyone will stay current on emergency procedures and to discover configuration issues or other problems with the radio system.

4.10.21 Configuring Selectable Group Scan

Section “ Group Scan in Connect Plus System” provides a detailed discussion of how Selectable Group Scan operates in Connect Plus. This section discusses how the SU is configured for Selectable Group Scan with MOTOTRBO Connect Plus Option Board CPS.

The following must be configured:

1. The individual that programs the SU must create the Group Scan list. A different scan list can be created for each Connect Plus zone. The Scan List has two columns, “Available” and “Members”, and two buttons, “Add” and “Remove”. There is a drop-down list of Connect Plus zones to the left side of the “Available” column. MOTOTRBO Connect Plus Option Board CPS automatically places a Group in the “Available” column when it has been assigned a Channel Selector Knob position (portable radio) or Channel Rocker position (mobile radio) in the zone selected via the drop-down list.

    a. To place a Group ID on the Configurable Group Scan list, the Group must be moved from the “Available” column to the “Members”” column on the Zone Scan tab.

    b. The Multigroup ID and the Site All Call ID will never appear in the “Available” column. This is unnecessary since the Connect Plus SU automatically responds to calls on these IDs.

c. The “Selected” Registration Group, the “Multigroup” (if configured in the SU) and the “Site All Call” appear in the “Members” column to remind the individual programming the SU that the radio always listens for these IDs. They cannot be removed from the “Members” column.

d. When the “Add” button is used to move a Group Contact from the “Available” column to the “Members” column, the Contact no longer appears in the “Available” column.

e. When the “Remove” button is used to move a Group Contact from the “Members” column, it will appear in the “Available” column if the Contact’s “zone of origin” is selected in the zone drop-down list. If the Contact’s “zone of origin” is not selected in the zone drop-down list, the removed Contact will not be displayed in the “Available” column.

f. The “Available” column will not display any Contact that has the same Contact Name as a contact already displayed in the “Members” Column”.

g. When moving a Contact from the “Available” Column to the “Members” column, Connect Plus checks to see whether the “Contact ID” (aka “Call ID”) is the same as another Contact already in the “Members” column. If so, the move is not allowed and Connect Plus CPS provides an error message.

h. To reduce confusion when configuring a Zone Scan List, the following guidelines are strongly recommended:

   i. If the same Contact Name is used in more than one zone contact list, it should be paired with the same Call ID.

   ii. If the same Call ID is used in more than one zone contact list, it should be paired with the same Contact Name.

i. Scan Talkback can be enabled/disabled via a Connect Plus CPS checkbox on the Zone Scan screen. For more information on the operation of Scan Talkback, see section titled, “Participating in Selectable Scan Calls”.

j. One Group from every Zone Scan List can be configured as the “Priority One” scan group and one Group can be configured as the “Priority Two” scan group. This can also be accomplished via the radio Scan menu, if the radio is display-equipped and has been enabled for “Edit List” via Connect Plus CPS. For more information, see section titled “Priority Monitor Scan”.

2. Once the scan list is configured, the radio user must have a way to enable and disable the Selectable Group Scan feature.

   a. The most common method is to configure a “Scan On/Off” button. This programmable button can be assigned to either a “short” or “long” button press. It is available for all radio models.

   b. In order for users of display radios to enable/disable the Selectable Group Scan feature via the menu, the “Scan” checkbox must be enabled in the “*Menu→Scan*” screen.

   c. Regardless of the method used to enable/disable the scan feature (programmable button or menu option), the current state (scan “on” or scan “off”) is applied to all Connect Plus zones with a selectable scan list and configured with the same Network ID. The Connect Plus SU will remember the current state (scan “on” or scan “off”) through a power cycle.

3. In order for the radio user to be able to edit the scan list via the menu, the “Edit List” checkbox on the “*Menu→Scan*” screen must be selected as well.

    a. When the “Edit List” option is enabled, the radio user has the ability (via the radio menu) to enable/disable scan functionality for individual scan list members. This is done by using the radio menu to scroll through the list of scan members.

    b. The scrollable scan list will show an entry for each Group alias that was moved from the “Available” column to the “Members” column with MOTOTRBO Connect Plus CPS. The scrollable scan list does not show Groups that are always & automatically scanned (such as the Multigroup ID and the Site All Call ID).

    c. An asterisk (*) denotes a scan list member that is currently active (meaning that the radio will scan for this ID when the scan feature is enabled).

    d. The absence of the asterisk indicates that the radio will NOT scan for this member (unless it happens to be SU’s currently registered Group).

    e. When a scan list member appears on the display, and the radio user presses “OK”, the radio provides a prompt to either “Enable” or “Disable” scan for the selected member (depending on the member’s current state).

    f. The radio user can also add groups to the zone scan list and delete groups from the zone scan list via the menu. This requires a display-equipped radio that is enabled for the Scan menu “Edit List” option. For more information on how to add or delete a scan list member via the menu, consult the MOTOTRBO Connect Plus User Guide for your radio model.

    g. The ability to toggle scan on and off for individual scan list members is available for any group on the selectable scan list, regardless of whether the group was added with Connect Plus CPS or whether it was added by the radio user via the menu.

4. The “Edit List” feature makes it possible for the radio user to disable scan for a specific list member if communications on that Group become a nuisance to the radio user. In doing so, the radio user should be aware of the following:

    a. This will not cause the radio to exit an ongoing call. However, it will prevent the radio from scanning into subsequent calls on this Group (assuming that it isn’t the SU’s registered Group) until the list member is enabled again.

    b. When a scan list member has been disabled via the menu, this setting is retained through a power cycle. The scan list member is not automatically re-enabled upon power-up.

Note: Because the editable scan list is only available to display radios, non-display units scan for <u>all</u> list members whenever Selectable Group Scan is enabled and the radio is registered to any network site. This is also true for display units that were not configured with the “Edit List” option.

4.10.22 Fleet Mapping Considerations for Other Call Features

The system designer should be familiar with the operation of other Connect Plus call features discussed in the System Feature Overview Section. These features include:

- Remote Monitor
- Radio Check

- Call Alert
- Radio Disable
- Radio Enable

Of the features listed above, only Call Alert can be initiated by a non-display or limited display radio (via a programmed "One Touch Call" button). All other features can only be initiated via the Menu, which requires a display radio.

When initiating one of these features via the menu, there are two ways to select the destination ID:

1. Select a Private Call Contact from the Zone Contact List as the Destination ID.
2. Enter the Destination Private Call ID via Manual Dial. This requires a radio keypad.

In most networks, the ability to initiate these features will be limited to supervisor radios. Connect Plus CPS programming and XRC programming (via the MOTOTRBO Connect Plus Network Manager) both play a role when implementing these features:

Initiating a Remote Monitor

SU Programming (Connect Plus CPS)	**Controller programming (Network Manager)**
Enable the Remote Monitor Menu option	Enable the "Remote Monitor Init" privilege on the SU record corresponding to the initiating radio.

Receiving a Remote Monitor

SU Programming (Connect Plus CPS)	**Controller programming (Network Manager)**
No special programming required	Enable the "Remote Monitor Receive" privilege on the SU record corresponding to the destination radio.

Initiating a Radio Check

SU Programming (Connect Plus CPS)	**Controller programming (Network Manager)**
Enable the Radio Check Menu option	Enable the "Radio Check Init" privilege on the SU record corresponding to the initiating radio.

Receiving a Radio Check

SU Programming (Connect Plus CPS)	**Controller programming (Network Manager)**
No special programming required	No special programming required.

Initiating a Call Alert

SU Programming (Connect Plus CPS)	**Controller programming (Network Manager)**
Enable the Call Alert Menu option	Enable the "Call Alert Init" privilege on the SU record corresponding to the initiating radio.

Receiving a Call Alert

SU Programming (Connect Plus CPS)	Controller programming (Network Manager)
No special programming required	No special programming required.

Disabling another SU

SU Programming (Connect Plus CPS)	Controller programming (Network Manager)
Enable the Radio Disable Menu option	Enable the "Radio Disable Init" privilege on the SU record corresponding to the initiating radio.

Being Disabled by another SU

SU Programming (Connect Plus CPS)	Controller programming (Network Manager)
No special programming required	Enable the "Radio Disable Receive" privilege on the SU record corresponding to the destination radio. This only applies to a Disable Command sent by another SU. The controller can disable any SU.

Enabling another SU

SU Programming (Connect Plus CPS)	Controller programming (Network Manager)
Enable the Radio Enable Menu option	Enable the "Radio Enable Init" privilege on the SU record corresponding to the initiating radio.

Being Enabled by another SU

SU Programming (Connect Plus CPS)	Controller programming (Network Manager)
No special programming required	Enable the "Radio Enable Receive" privilege on the SU record corresponding to the destination radio. This only applies to an Enable Command sent by another SU. The controller can enable any SU.

4.10.23 Fleet Mapping Considerations for OTA File Transfer

An important Fleet Mapping decision is whether an SU should be enabled to receive Option Board Firmware Files and Network Frequency Files over-the-air (OTA). This is controlled via Connect Plus CPS programming. To enable the option, check the box labeled "Enable OTA File Transfer". This setting is configurable for each Connect Plus zone.

By default, this codeplug option is NOT enabled. Prior to enabling the option, the System Administrator should be very familiar with how the feature operates. For more information, see the discussion on OTA File Transfer in the System Feature Overview Section.

Note: This Connect Plus CPS setting does not affect OTA Transfer of the Option Board codeplug. The System Administrator grants permission for Option Board codeplug OTA transfer to take place by acknowledging a Network Manager message when uploading a new Option Board codeplug for a specific radio.

4.11 Configurable Timers: Connect Plus CPS

The following table discusses configurable timers for the Connect Plus Option Board. These timers are configured with Connect Plus Customer Programming Software (Connect Plus CPS).

Timer Name	Description	Notes
Long Press Duration	Sets the duration a button is required to be pressed (and held down), for it to be interpreted as a long press.	Set on the “Buttons Screen” and applies to all Connect Plus zones
Menu Hang Time	Sets the amount of time that the radio remains in the menu mode, after which the radio reverts back to the Home screen. If the duration is set to 0, the radio remains infinitely in this mode.	Set on the “Menu Screen” and applies to all Connect Plus zones
PTT Time Out Time	The Time-Out Timer (TOT) is the duration that the radio can continuously transmit before the transmission is automatically terminated by the radio. PTT must be released (and pressed again) before the radio will make another attempt to transmit.	Configurable per Connect Plus zone
Remote Monitor Duration Time	Sets the duration that this radio will automatically transmit with microphone open when it is being remote monitored. The radio user will not be aware that he/she is being monitored. To prevent this radio from being remote monitored, uncheck the “Remote Monitor Receive” checkbox on the User Record in the Connect Plus controller.	Configurable per Connect Plus zone
Unconfirmed File Xfer Dwell Time	During Unconfirmed File Transfer this value determines how long the radio will remain on the trunk-to timeslot without decoding any valid file packets. If the timer expires and no valid packet is decoded, the radio returns to the Control Channel timeslot. If the OTA File Transfer was for Option Board Firmware or the Network Frequency File, the Option Board starts its “File Transfer Attempt Interval Time” upon returning to the Control Channel timeslot.	Configurable per Connect Plus zone
File Transfer Attempt Interval Time	When the radio has been involved in an Option Board Firmware or Network Frequency File OTA Transfer, and it leaves the trunk-to timeslot with an incomplete file (for any reason), the radio starts the File Transfer Attempt Interval Time. The timer must expire before the radio will automatically attempt to resume the file transfer.	Configurable per Connect Plus zone
CSBK Roam Delay Time	Determines how long the radio will continue to listen to the current Control Channel when it doesn’t decode any valid Control Channel messages. If the timer expires, and the radio hasn’t decoded a valid message, the radio starts to search.	Configurable per Connect Plus zone

Roam Dwell Time	When searching for a site, this is the amount of time the radio remains on each search frequency waiting to detect digital signaling. If digital signaling is detected, the radio waits an additional time to identify the site (via control channel messaging) and measure RSSI. If this time expires and the radio has not detected digital signaling, it then proceeds to search the next frequency on the list.	Configurable per Connect Plus zone
Reacquire Time	When the radio loses acceptable signal from its current site and begins searching, a countdown timer is set to this value. If during the search process the radio again finds the site it just lost and this timer has not expired and the radio has not attempted to register at another site, the radio returns to the registered state without transmitting a registration request to the site. This feature can help reduce registration traffic on the control channel and extend portable battery life.	Configurable per Connect Plus zone
BSI Wait Time	If the radio decodes a control channel message indicating that the control channel repeater is getting ready to start analog Base Station Identification, the Option Board will wait this amount of time prior to looking for another site (however, the radio will still display “Searching” during BSI transmission). If BSI concludes prior to the expiration of this timer, the Option Board remains with the same site and control channel. Because the repeater reverts to analog mode during analog BSI, it is important to note that analog BSI on the control channel repeater will cause significant operational problems to radios using the site and should be avoided if at all possible. During analog BSI, calls and registration cannot be initiated, and the control channel sends no messages for calls in-progress. If the control channel repeater must do analog BSI, this value should be set to the length of time required to send the Morse Code identification, plus an extra 5 seconds to allow adequate time for the digital-to-analog and analog-to-digital transitions.	Configurable per Connect Plus zone
RSSI Roam Delay Time	The radio starts this timer when the received signal strength from the control channel drops to RSSI minimum or lower. If the signal strength rises above RSSI Minimum before the timer expires, the radio stops the timer. If the timer expires and the received signal strength is still at this value or lower, the radio starts to search.	Configurable per Connect Plus zone

(Emergency) Hot Mic Duration	If the Mode is selected as Emergency Call with Voice to Follow, after the SU synchs with the assigned repeater and slot, the Hot Mic feature is activated whereby the radio automatically begins transmitting voice for the duration indicated by the Hot Mic Duration. There is no need to press the Push-To-Talk (PTT) button during this time in order to transmit voice. The transmission is sent as Emergency key-up. Once this duration expires, the radio automatically dekeys (unless the radio user has manually pressed PTT prior to expiration of the timer).	
(Tilt Alarm) Alarm Tone Delay Time	Determines how long the radio can remain tilted beyond the configured Activation Angle before the radio begins to play the Alert Tone.	Portable Radio Only. Requires purchase of Man Down feature.
(Tilt Alarm) Alarm Activation Time	Determines how long the Alert Tone will play before the radio automatically initiates an Emergency Call.	Portable Radio Only. Requires purchase of Man Down feature.
(Anti-Movement Alarm) Alarm Tone Delay Time	Determines how long the radio can remain motionless before the radio begins to play the Alert Tone.	Portable Radio Only. Requires purchase of Man Down feature.
(Anti-Movement Alarm) Alarm Activation Time	Determines how long the Alert Tone will play before the radio automatically initiates an Emergency Call.	Portable Radio Only. Requires purchase of Man Down feature.
(Movement Alarm) Alarm Tone Delay Time	Determines how long the radio can remain in motion before the radio begins to play the Alert Tone.	Portable Radio Only. Requires purchase of Man Down feature.
(Movement Alarm) Alarm Activation Time	Determines how long the Alert Tone will play before the radio automatically initiates an Emergency Call.	Portable Radio Only. Requires purchase of Man Down feature.

4.12 Configurable Timers: Connect Plus Network Manager

The following table discusses configurable timers for the XRC Controller. These times are configured with the MOTOTRBO Connect Plus Network Manager Software.

Timer Name	Description	Notes
Multisite Ping Interval	Defines the ping interval the controller uses to verify the communications link with other network sites. Each site pings only the higher-numbered sites at this interval.	Site Configuration Screen
Group Call Hang Time	The Group Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Group Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See section “Setting Repeater Hang Times in Connect Plus” in Connect	Site Configuration Screen

	Plus, for more information.	
Private Call Hang Time	The Private Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Private Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See section "Setting Repeater Hang Times in Connect Plus" in Connect Plus, for more information.	Site Configuration Screen
Emergency Call Hang Time	The Emergency Call Hang Time value configured with MOTOTRBO CPS will be overwritten with the Emergency Call Hang Time configured with the MOTOTRBO Connect Plus Network Manager. See sections "Setting Repeater Hang Times in Connect Plus" and "Programming the Repeater's Emergency Call Hang Time" for more information.	Site Configuration Screen
Arbitration Time	Upon receiving IP voice packets, the controller waits the arbitration time prior to forwarding the voice packets to the repeater for transmission. In the event of near-simultaneous key-ups at different sites during the same call, arbitration increases the chances that the same audio will be heard at all sites involved in the call. This timer is only available when the XRC controller is enabled for multisite operation.	Site Configuration Screen
CSBK Call Retry Interval	Determines the interval that must expire before the controller initiates a CSBK Call Retry	Site Configuration Screen
SU Inactivity Time	This timer is set per controller, but it is tracked separately for each registered SU. The Timer is reset whenever the controller detects a transmission from the SU. This includes registrations, Call Requests, Voice Transmissions, etc. If the timer expires, and the controller shows that the SU is still registered to the site, the Controller will send the SU a "Controller Initiated Radio Check". If the SU answers the Radio Check, the controller resets the SU Inactivity Time and leaves the unit registered to the site. If the SU does not respond to the Radio Check, the controller will re-send the Radio Check as determined by the "CSBK Call Retry" Parameter. If the SU fails to respond to any of the Radio Checks, the Controller will de-register the SU from the site. This helps conserve resources by detecting which SU's are no longer available or in range to receive calls.	Site Configuration Screen
BSI Interval	This timer controls how often the repeater will send its Base Station Identification (BSI), which is also called CWID. The ID itself is set in the repeater, not in the Controller. The repeater can also be configured to send analog or digital BSI. It is important to note that analog BSI (CWID) on the control channel repeater will cause significant operational problems to radios using the site	This is settable per repeater. If a repeater should not send CWID, it should not be entered on the repeater list. If it is on the list for some reason, the BSI interval

	and should be avoided if at all possible.	should be set to zero.
Time to Beacon	Determines how long the controller will "beacon" a special control channel message to inform SU's of file availability. This time must be equal to or greater than the "Time to Dedicate". Anytime that "Time to Dedicate" has expired, but "Time to Beacon" has not, the file is still available – but by request only. A setting of 65,535 minutes tells the controller that the Beacon message should never expire.	OTA File Upload Screen
Time to Dedicate	Determines how long the repeater and timeslot configured above will be used for the dedicated channel file transfer. During this time, the timeslot cannot be used for other calls. SU's may join or leave the dedicated channel transfer at various times (the radio user can cancel out of the transfer). A setting of 65,535 minutes tells the controller that the dedicated channel transfer should never expire. Important: "Time to Beacon" must be equal to or greater than the "Time to Dedicate".	OTA File Upload Screen

4.13 Backup Power Source

Emergency backup power systems usually consist of two components: an Uninterrupted Power Supply (UPS) and a generator. This section only describes the UPS; the selection of the generator is beyond the scope of this document. A UPS can serve a number of purposes such as filtering out power events, conditioning and providing power if primary power source fails. On the average, the time a UPS is expected to do this is under five minutes which gives enough time to shut down equipment and for the backup power generator to take over the load.

Depending on your configuration and needs, the following areas require different emphasis:
• Surge Suppression
• Power Conditioning
• Battery Backup

It is required that the XRC and its supporting network equipment (i.e. router, switches, and repeaters) are backed up by UPS. The XRC is a 50 W unit. It is recommended to check the power requirements of other devices (such as repeaters and network equipment) when calculating the required capacity of a UPS system.

To determine the UPS capacity:

1. List all equipment to be protected by the UPS.
2. Write down the voltage and amperage for each device.
3. Multiply the voltage by the amperage of each device to calculate the Volt/Amps (VA).

NOTE: Some equipment may be marked with a power consumption measured in Watts. To convert Watts to VA, simply divide Watts by 0.65 (for a power factor of 0.65), or multiply by 1.54. The power factor refers to the relationship between the apparent power (volt-amps) required by the device and the actual power (watts) produced by the device.

4. Total the VA for all devices you want to protect with the UPS.

5. Multiply the subtotal found in Step 4 by 0.25. This number takes into account room for future growth. This growth factor allows for a 5% rate of growth for each year over a five-year period.

6. Add the results of steps 4 and 5 to get the Required VA. Now you can select the appropriate UPS model by choosing a model that has a VA rating at least as large as the Required VA that you calculated.

Standard UPS units for the XRC Controller and networking equipment are included in the Price Books.

4.14 External NTP Source (Time Master)

The NTP (Network Time Protocol) is used between the controllers to keep their clocks synchronized. Usually, in a multisite Connect Plus system one of the XRC controllers is designated as the system *NTP Server* through the Network Manager.

Since NTP is a standard protocol, external devices can also provide time synchronization service. Connect Plus has been tested and verified with the following GPS-based NTP Time Servers:

- TRAK 8835 Time and Frequency GPS Clock
- Unison GPS Network Time Server

When using an external NTP time server, the NTP Server (IP) Address must be provisioned in the XRC/XRT Site Configuration screen.

4.15 Grounding and Surge Suppression

Proper site grounding and surge suppression are important considerations for safe and reliable operation of the Connect Plus trunking system. Refer to the Motorola Quality Standards Fixed Network Equipment Installation Manual R56 [5] for more details.

Appendix A Acronyms

ACK	Acknowledgment
ADK	Application Development Kit
ADSL	Asymmetric Digital Subscriber Line
ARS	Automatic Registration Service
ATB	All Trunks Busy (no traffic channel available)
BSI	Base Station Identification
CAI	Common Air Interface
CPS	Customer Programming Software
CSA	Canadian Standards Association
CSBK	Control Signaling Block
CUCM	Cisco Unified Communications Manager (CallManager)
CWID	Continuous Wave Identification (same as BSI)
DMR	Digital Mobile Radio (ETSI standard)
DSL	Digital Subscriber Line
ESN	Electronic Serial Number
ETCA	Enhanced Traffic Channel Access
ETSI	European Telecommunications and Standard Institute
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
GLONASS	GLObal NAvigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HTTP	Hyper Text Transport Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LRRP	Location Request Response Protocol
MCDD	Multi-Channel Device Driver
NAK	Negative ACK (acknowledgment)
OTA	Over the Air
PDU	Protocol Data Unit
PTT	Push To Talk
QoS	Quality of Service
PSN	Physical Serial Number
RDAC	Repeater Diagnostics and Control
RSSI	Received Signal Strength Indication
RRP	Remote Repeater Programming
SAPR	Site Access and Permanent Registration
SIT	Subscriber Inactivity Timer
SMTP	Simple Mail Transport Protocol
SU	Subscriber Unit
TOT	Time Out Timer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TMS	Text Messaging Service
UDP	User Datagram Protocol
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
VPN	Virtual Private Network

VOX	Voice Operated Transmission
WAN	Wide Area Network
XML	Extensible Mark-up Language

Appendix B Sample (Suggested) Network Topology

Figure B 1 shows a multisite configuration with 6 Connect Plus sites with 3 repeaters per site, providing 5 trunked channels. The network topology is private LAN/WAN, which does not require any special port forwarding or network address translation. Each XRC controller can directly communicate with the other site controllers via their configured IP addresses. The IP addresses are chosen from the private IPv4 address space and can be used with any Connect Plus installation, because IP packets originating from the Connect Plus devices are not routed to the public Internet, and conversely, no device in the public Internet domain can directly send IP packets targeting a device with a private IP address.

The setup in Figure B 1 also shows managed network switches with at least 4 ports available for the Connect Plus equipment. Note that although the switches have assigned IP addresses this is not required and the only purpose for such setting is to allow remote IP access to the switch for configuration purposes. The reader should not confuse a switch with a router, which usually is the default IP gateway for the devices that reside on router's designated subnet.

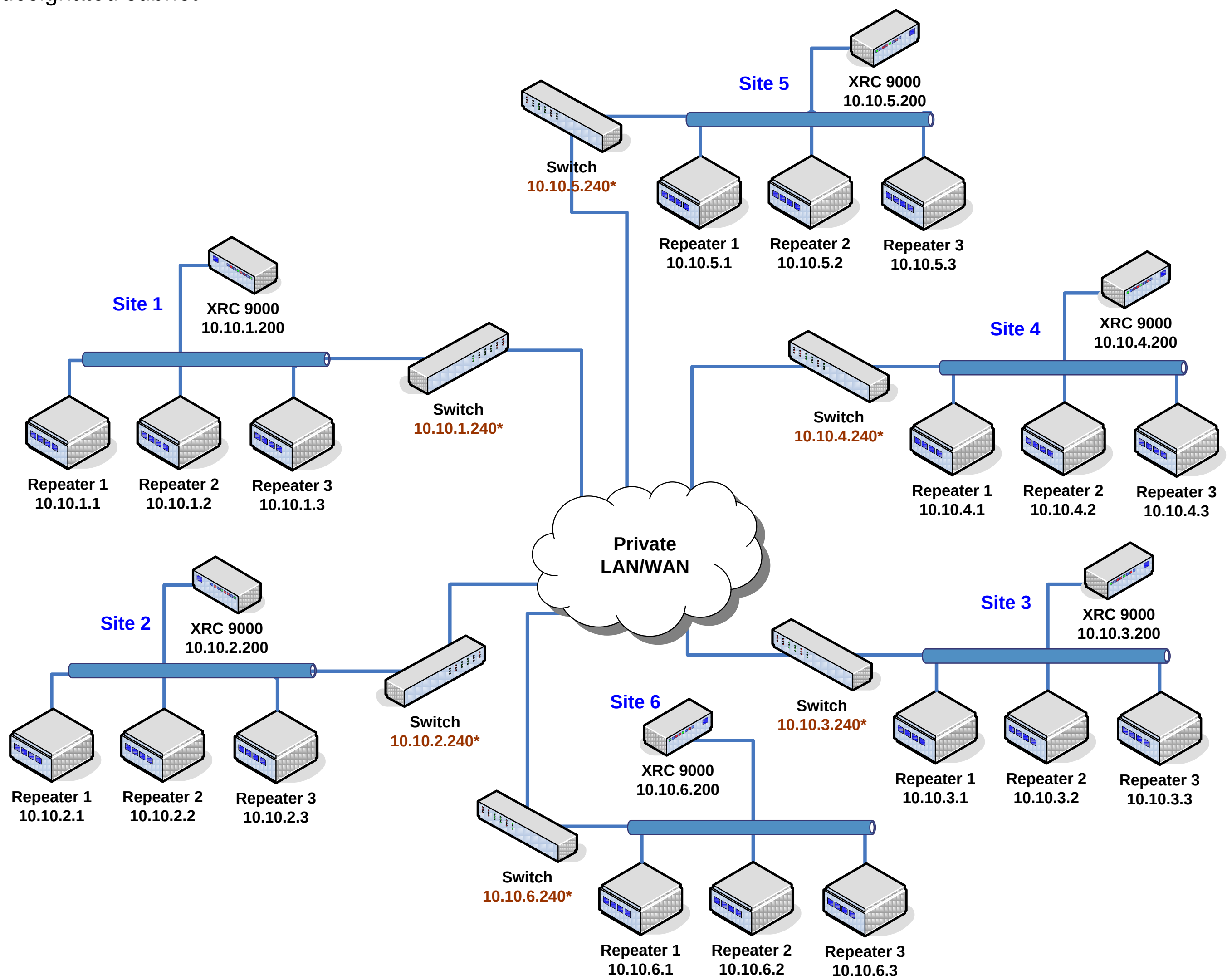


Figure B 1 Sample Network Topology with Private IP Plan

Appendix C Fleetmap Strategy to Facilitate Merging Multiple Systems

There are certain guidelines that should be followed when setting up radios in separate multi-site systems that may be linked together at a later date. The guidelines are related to how the radio fleet map is designed by the System Manager and how this fleet map information is entered in the Connect Plus Network Manager (NM). While the guidelines described in this section are specifically written for separate multisite systems that may be linked together in the future, many of the same principles also apply to single site systems that may be linked together as a multisite system at some future date.

The fleet map design guidelines are intended to minimize radio programming and NM updates at the time of linking one or more systems together.

GUIDELINES

Basically, radio, talk group, and Multigroup ID assignment should be looked at as if there was one single system from the beginning. Let's assume as an example a customer is setting up 2 separate systems today: **System A** (5 RF sites) and **System B** (4 RF sites) and is planning to link all 9 sites at a later date to form **System C**.

1) **Do not duplicate radio ID's**.

Radio IDs should be unique across all systems. For example: if user ID 05 is being used in **System A**, then user ID 05 should not be used in **System B**. This practice will minimize radio programming and NM database updates at the time of linking the systems.

2) **Do not duplicate Group ID's.**

Group IDs should be unique across all systems. For example: if group ID 01 is being used in **System A**, then group ID 01 should not be used in **System B**. This practice will minimize radio programming and NM database updates at the time of linking the systems.

3) **Do not duplicate Multigroup ID's.**

Multigroup ID's should be unique across all systems. Example, if customer X is using Multigroup 10000 on **System A** then multi group 10000 should not be used on **System B**. This practice will minimize radio programming and NM database updates at the time of linking the systems.

One possibility for this 2 system scenario for example, is to use ODD IDs for **System A** and EVEN IDs for **System B**.

4) **Site ID's must be unique.**

Ensure each site ID is unique after linking both **Systems A** and **B** together.

This is how the site ID assignment may look on this example before linking the systems.

System A	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6
Site ID	1	2	3	4	5	-

System B	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6
Site ID	1	2	3	4	-	-

This is how the site ID assignment will look after linking the 2 systems.

System C	Site 1	Site 2	Site 3	Site 4	Site 5	Site 6	Site 7	Site 8	Site 9
Site ID	1	2	3	4	5	6	7	8	9

5) **Use same Network ID (NID) for all controllers.**

Having all controllers in **System A** and **System B** with the same NID from the beginning ensures that the XRC controllers will not need to be updated with the final NID.

Similarly, having all radios with the same NID from the beginning ensures that the radios will not be required to be brought in for reprogramming with the new NID. A new frequency file will have to be sent over-the-air (OTA) in order to let the radios know about the new sites available in the final **System C** configuration.

The Network ID is not a configurable parameter in the Network Manager. If all controllers should have the same Network ID, this should be communicated at time of purchase. If this is not known at time of purchase, a controller's Network ID can be changed at a later date, but it will necessitate the reprogramming of the subscriber radios.

6) **Network Manager User database.**

It is expected that some database updates are required when joining **System A** and **System B** together but these updates could be minimized by following some simple guidelines. **System A** database may be transferred to the new sites coming from **System B** (sites 6, 7, 8, and 9 on this example) as a starting point. Final system database must be updated to reflect all new subscriber and site records. The last step will be to enable the EVEN IDs so that all users can utilize **System C**.

Example for Radios IDs (same could apply to group and Multigroup IDs):

Initial Setup
Both system databases are initially independent. ODD IDs are being used for **System A** and EVEN IDs are being used for **System B**.

System A User Database	**System B** User Database
ODD IDs Enabled	**EVEN IDs Enabled**

Let's assume **System A** database will be the one used for final configuration of **System C**. In the time prior to linking the 2 systems together, **System A** database can be prepared in advance by creating the EVEN IDs from **System B**, but keeping them disabled.

Interim Setup
Both system databases are still independent, but now (EVEN) ID's from **System B** exist on **System A** database although they are disabled.

System A User Database	**System B** User Database
ODD IDs Enabled **EVEN IDs Disabled**	**EVEN IDs Enabled**

At the time of linking the 2 systems together all EVEN IDs in **System A** database will be enabled and as a result we will have a **System C** database ready.

Final Setup
System A database now includes all combined ID's required, so it can be considered the final **System C** database.

System C User Database
ODD IDs Enabled
EVEN IDs Enabled

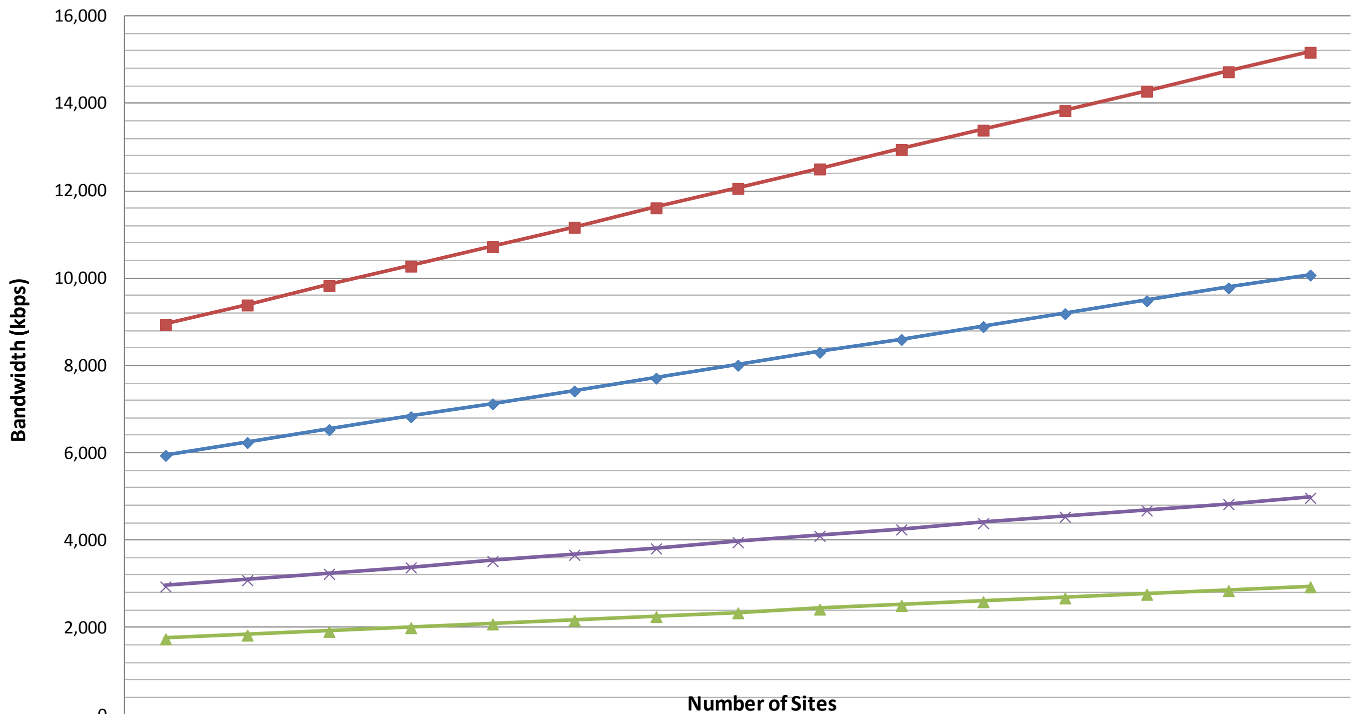
Alternate option for user database management

If the two (or multiple) systems have different frequencies, this greatly reduces the chances that radios will attempt to register on the wrong system (prior to combining the systems). Because of this, you can use an alternate method managing both systems by using one system as the main entry point for all user information.

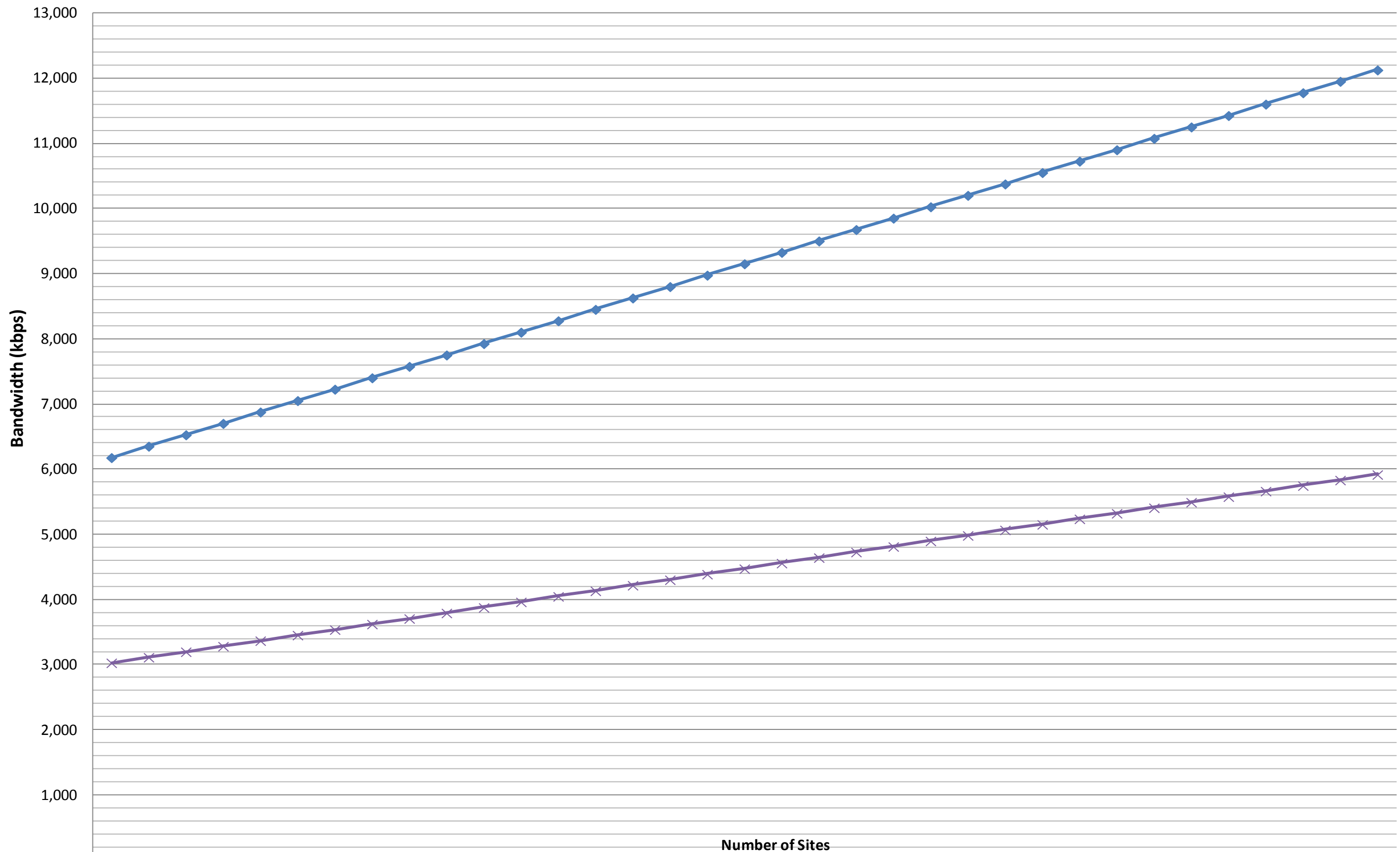
Example, Enter all the users information for BOTH systems on **System A**, make a back up copy of the user database for **System A**. Access the Network Manager for **System B**, restore the user database from **System A** to **System B**. Both systems will now have the complete user database for all users. When the two systems are connected together to form **System C**, the databases will already be common between the two systems.

Note: Although you are using a common database for both Systems A and B guidelines 1, 2, and 3 still apply: you need to keep every radio, group, and Multigroup ID unique across all systems.

Appendix D Bandwidth Requirements for Multisite System Beyond 20 Sites



	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
3 repeaters	1755	1840	1925	2010	2095	2180	2265	2350	2435	2520	2605	2690	2775	2860	2945
5 repeaters	2955	3100	3245	3390	3535	3680	3825	3970	4115	4260	4405	4550	4695	4840	4985
10 repeaters	5955	6250	6545	6840	7135	7430	7725	8020	8315	8610	8905	9200	9495	9790	10085
15 repeaters	8955	9400	9845	10290	10735	11180	11625	12070	12515	12960	13405	13850	14295	14740	15185



	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
3 repeaters	3030	3115	3200	3285	3370	3455	3540	3625	3710	3795	3880	3965	4050	4135	4220	4305	4390	4475
6 repeaters	6180	6355	6530	6705	6880	7055	7230	7405	7580	7755	7930	8105	8280	8455	8630	8805	8980	9155

	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70
3 repeaters	4560	4645	4730	4815	4900	4985	5070	5155	5240	5325	5410	5495	5580	5665	5750	5835	5920
6 repeaters	9330	9505	9680	9855	10030	10205	10380	10555	10730	10905	11080	11255	11430	11605	11780	11955	12130

Appendix E Ethernet Switch Specifications

The following performance specifications are recommended when selecting Ethernet switch model for Connect Plus system installations.

Latency	< 5 µs (64-byte packets)
Throughput per port	200 Kpps (64-byte packets)
MAC address table size	4,000 entries
IGMP support (v2 or higher)	IGMP snooping